AVG Internet Security 2012

Manuale per l'utente

Revisione documento 2012.20 (3/29/2012)

Sommario

1. Introduzione

Questa guida per l'utente fornisce la documentazione completa relativa a **AVG Internet Security 2012**.

Grazie ai diversi livelli di protezione per tutte le attività svolte in linea offerti da AVG Internet Security 2012, il furto d'identità, i virus o i siti pericolosi non sono più un problema. Con le funzionalità Tecnologia di protezione cloud AVG e Rete di protezione della community AVG incluse nel prodotto, le informazioni sulle minacce più recenti vengono raccolte e condivise con la community per fornire una protezione ottimale:

- Acquisti e operazioni bancarie in linea sicuri con AVG Firewall, Anti-Spam e Identity Protection
- Protezione del PC durante l'uso dei social network con Protezione dei social network AVG
- Navigazione e ricerche in totale sicurezza con la protezione in tempo reale di LinkScanner

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG Internet Security 2012 è destinato alla protezione delle workstation che eseguono i seguenti sistemi operativi:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 e x64, tutte le edizioni)
- Windows 7 (x86 e x64, tutte le edizioni)

(ed eventualmente Service Pack successivi per sistemi operativi specifici)

Nota*: il componente ID Protection non è supportato in Windows XP x64. Su questo sistema operativo è possibile installare AVG Internet Security 2012, ma solo senza il componente IDP.*

2.2. Requisiti hardware minimi e consigliati

Requisiti hardware minimi per **AVG Internet Security 2012**:

- CPU Intel Pentium da 1,5 GHz
- 512 MB di memoria RAM
- 1000 MB di spazio libero sul disco rigido (per l'installazione)

Requisiti hardware consigliati per **AVG Internet Security 2012**:

- CPU Intel Pentium da 1,8 GHz
- 512 MB di memoria RAM
- 1550 MB di spazio libero sul disco rigido (per l'installazione)

3. Processo di installazione di AVG

Dove posso trovare il file di installazione?

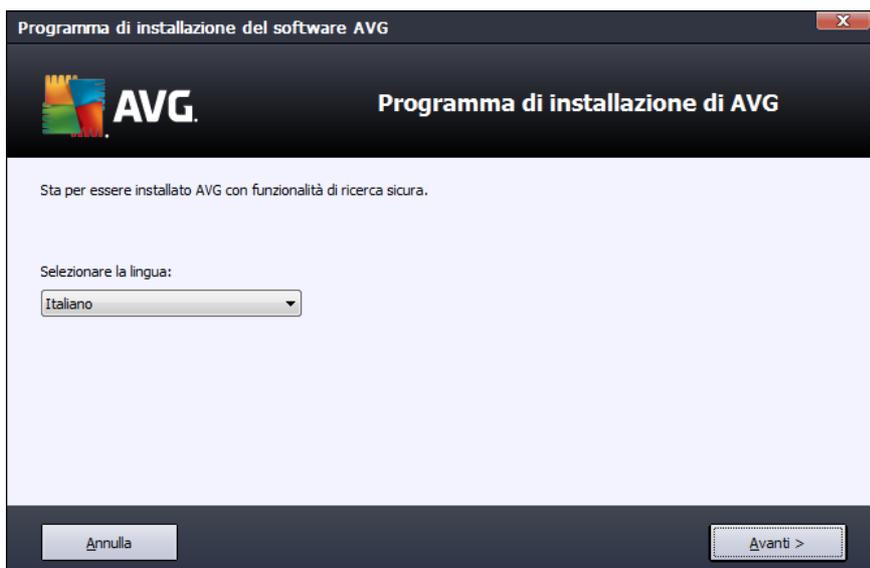
Per installare **AVG Internet Security 2012** nel computer è necessario disporre del file di installazione più recente. Per assicurarsi di installare la versione aggiornata di **AVG Internet Security 2012**, si consiglia di scaricare il file di installazione dal sito Web di AVG (http://www.avg.com/). La sezione ***Centro di assistenza / Download*** fornisce una panoramica strutturata dei file di installazione per ciascuna edizione di AVG.

In caso di dubbi sui file da scaricare e installare, è possibile utilizzare il servizio ***Seleziona prodotto*** disponibile nella parte inferiore della pagina Web. Tramite le risposte a tre semplici domande il servizio definisce i file necessari. Fare clic sul pulsante ***Procedi*** per visualizzare l'elenco completo dei file per il download personalizzati in base alle esigenze specifiche.

Com'è strutturato il processo di installazione?

Dopo aver scaricato e salvato il file di installazione sul disco rigido, è possibile avviare il processo di installazione. L'installazione è una sequenza di finestre di dialogo semplici e chiare. Ciascuna finestra di dialogo descrive brevemente come procedere in ciascuna fase del processo di installazione. Di seguito viene fornita una descrizione dettagliata di ciascuna finestra di dialogo:

3.1. Finestra introduttiva: selezione della lingua

Il processo di installazione comincia con la finestra di dialogo ***Benvenuti nel programma di installazione di AVG***:

In questa finestra di dialogo è possibile selezionare la lingua utilizzata per il processo di installazione. Nell'angolo destro della finestra di dialogo fare clic sulla casella combinata per visualizzare il menu a discesa della lingua. Selezionare la lingua desiderata. Il processo di

installazione procederà quindi nella lingua prescelta.

Attenzione: in questa fase viene selezionata solo la lingua per il processo di installazione. L'applicazione AVG Internet Security 2012 verrà installata nella lingua selezionata e in lingua inglese, lingua che viene installata automaticamente. Tuttavia, è possibile installare più lingue e utilizzare AVG Internet Security 2012 in qualsiasi di queste lingue. Verrà richiesto di confermare la selezione di lingue alternative in una delle seguenti finestre di dialogo di installazione denominata Opzioni personalizzate.

3.2. Finestra introduttiva: contratto di licenza

Nel passaggio successivo, la finestra di dialogo ***Benvenuti nel programma di installazione di AVG*** fornisce il testo completo del Contratto di licenza AVG:

Leggere con attenzione l'intero testo. Per confermare che il contratto è stato letto e accettato, selezionare il pulsante ***Accetto***. Se non si accettano i termini del contratto di licenza, fare clic sul pulsante ***Rifiuta***. Il processo di installazione verrà interrotto immediatamente.

Informativa sulla privacy di AVG

Oltre al Contratto di licenza, questa finestra di dialogo di installazione offre ulteriori informazioni circa l'Informativa sulla privacy di AVG. Nell'angolo inferiore sinistro della finestra di dialogo è disponibile il collegamento ***Informativa sulla privacy di AVG***. Selezionarlo per visualizzare il sito Web di AVG (http://www.avg.com/) in cui è disponibile il testo completo dell'Informativa sulla privacy di AVG.

Pulsanti di controllo

Nella prima finestra di dialogo di installazione, sono disponibili solo due pulsanti di controllo:

- ***Versione stampabile*** : fare clic per stampare il contratto di licenza di AVG completo.
- ***Rifiuta***: fare clic per rifiutare il Contratto di licenza. Il processo di installazione verrà chiuso immediatamente. **AVG Internet Security 2012** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.
- ***Accetta***: fare clic per confermare che il Contratto di licenza è stato letto e accettato. L'installazione continuerà con la successiva finestra di dialogo.

3.3. Attiva la licenza di AVG

Nella finestra di dialogo ***Attiva la licenza di AVG*** viene richiesto di immettere il numero di licenza nel campo di testo fornito:

Dove è possibile reperire il numero di licenza

Il numero di vendita è disponibile sulla custodia del CD presente nella confezione di **AVG Internet Security 2012**. Il numero di licenza sarà contenuto nel messaggio e-mail di conferma ricevuto dopo l'acquisto in linea di **AVG Internet Security 2012**. È necessario digitare il numero esattamente come viene indicato. Se il numero di licenza è disponibile nel formato digitale (*contenuto nel messaggio e-mail*), si consiglia di utilizzare il metodo "copia e incolla" per immetterlo.

Come utilizzare il metodo Copia e incolla

L'uso del metodo ***Copia e incolla*** per immettere il numero di licenza **AVG Internet Security 2012** nel programma assicura un'immissione corretta. Procedere come segue:

- Aprire il messaggio e-mail che contiene il numero di licenza.

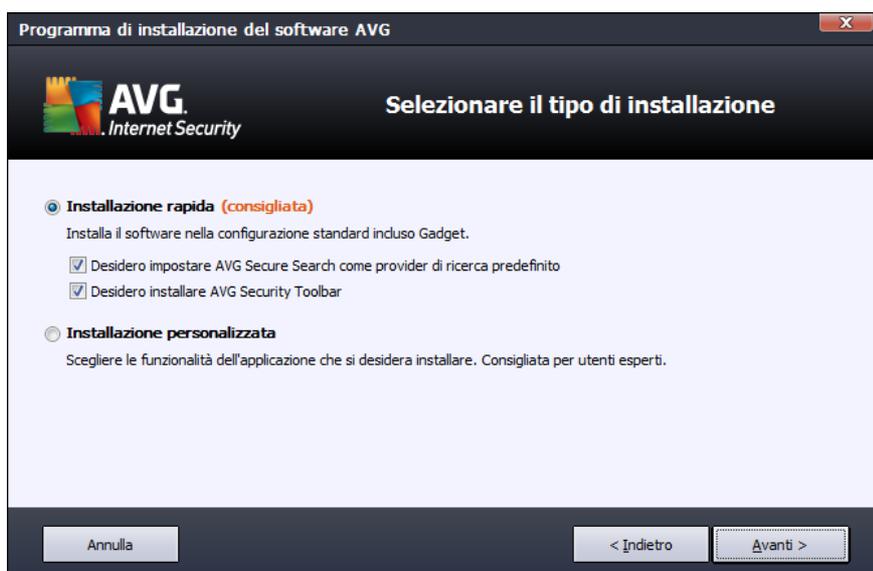
- Posizionare il cursore all'inizio del numero di licenza, premere il pulsante sinistro del mouse e, mantenendolo premuto, fare scorrere il cursore sul numero di licenza, quindi rilasciare il pulsante. Il numero viene evidenziato.
- Tenere premuto ***Ctrl***, quindi premere ***C***. Questa operazione copia il numero.
- Fare clic nella posizione in cui si desidera incollare il numero copiato.
- Tenere premuto ***Ctrl***, quindi premere ***V***. Questa operazione incolla il numero nella posizione selezionata.

Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo di impostazione, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire subito dal processo di installazione. **AVG Internet Security 2012** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.
- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo di installazione.

3.4. Selezionare il tipo di installazione

La finestra di dialogo ***Selezionare il tipo di installazione*** offre due opzioni di installazione: ***Installazione rapida*** e ***Installazione personalizzata***:

Installazione rapida

Per la maggior parte degli utenti è consigliabile scegliere l'***installazione rapida*** standard che consente di installare **AVG Internet Security 2012** in modalità completamente automatica con le impostazioni predefinite dal produttore del software, incluso AVG Gadget. Questa configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità di modificare la configurazione, sarà possibile farlo direttamente nell'applicazione **AVG Internet Security 2012**.

All'interno di questa opzione vengono visualizzate due caselle di controllo pre-confermate ed è consigliabile lasciarle entrambe selezionate:

- ***Desidero impostare AVG Secure Search come provider di ricerca predefinito***: lasciare selezionata l'opzione per confermare che si desidera utilizzare il motore AVG Secure Search, che funziona insieme al componente Link Scanner per assicurare la massima protezione in linea.

- ***Desidero installare AVG Security Toolbar***: lasciare selezionata l'opzione per installare AVG Security Toolbar, che assicura la massima protezione durante l'esplorazione di Internet.

Fare clic su ***Avanti*** per passare alla finestra di dialogo successiva Installa AVG Security Toolbar.

Installazione personalizzata

L'***installazione personalizzata*** deve essere utilizzata solo da utenti esperti che hanno valide ragioni per installare **AVG Internet Security 2012** con impostazioni non standard, ad esempio per soddisfare specifici requisiti di sistema.

Se si decide di utilizzare questa opzione, una nuova sezione chiamata ***Cartella di destinazione*** verrà visualizzata nella finestra di dialogo. Qui è possibile specificare il percorso in cui **AVG Internet Security 2012** deve essere installato. Per impostazione predefinita, **AVG Internet Security 2012** verrà installato nella cartella Programmi nell'unità C:, come indicato nel campo di testo della finestra di dialogo. Se si desidera modificare questo percorso, utilizzare il pulsante ***Sfoglia*** per visualizzare la struttura dell'unità e selezionare la cartella appropriata. Per ripristinare la destinazione predefinita dal fornitore del software, utilizzare il pulsante ***Predefinita***.

Premere quindi il pulsante ***Avanti*** per passare alla finestra di dialogo Opzioni personalizzate.

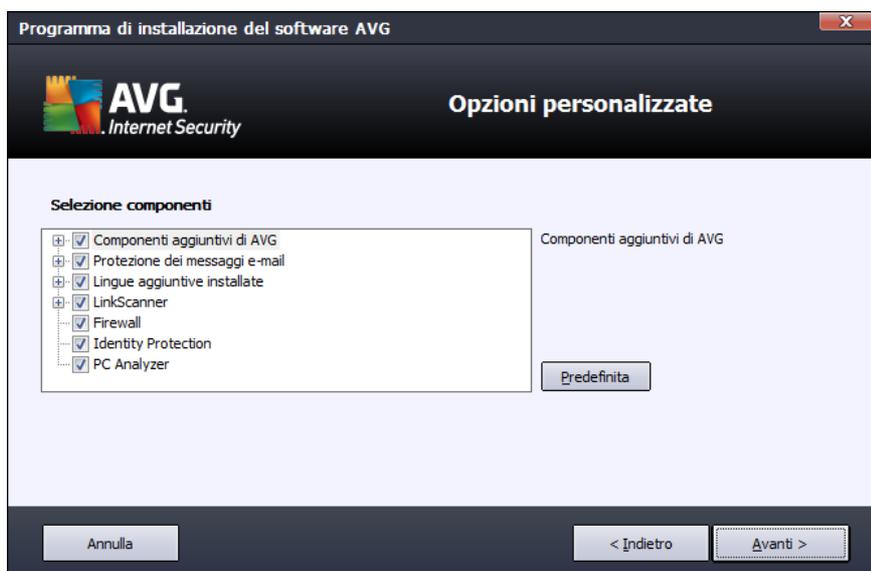
Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo di impostazione, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire subito dal processo di installazione. **AVG Internet Security 2012** non verrà installato.

- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.
- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo di installazione.

3.5. Opzioni personalizzate

La finestra di dialogo ***Opzioni personalizzate*** consente di impostare parametri di installazione dettagliati:

La sezione ***Selezione componenti*** visualizza una panoramica di tutti i componenti di **AVG Internet Security 2012** che è possibile installare. Se le impostazioni predefinite non sono adeguate alle esigenze specifiche, è possibile rimuovere/aggiungere determinati componenti.

È tuttavia possibile eseguire la selezione solo tra i componenti inclusi nell'edizione di AVG che è stata acquistata.

Evidenziare una voce dell'elenco ***Selezione componenti*** per visualizzare una breve descrizione del relativo componente nella parte destra della sezione. Per informazioni dettagliate sulla funzionalità di ciascun componente, consultare il capitolo Panoramica dei componenti di questo documento. Per ripristinare la configurazione predefinita dal fornitore del software, utilizzare il pulsante ***Predefinita***.

Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo di impostazione, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire subito dal processo di installazione. **AVG Internet Security 2012** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.

- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo di installazione.

3.6. Installa AVG Security Toolbar

Nella finestra di dialogo ***Installa AVG Security Toolbar*** è possibile decidere se installare o meno AVG Security Toolbar. Se non si modificano le impostazioni predefinite, questo componente verrà installato automaticamente nel browser Web (*i browser supportati al momento sono Microsoft Internet Explorer 6.0 o versione successiva e Mozilla Firefox 3.0 o versione successiva*) per offrire una protezione in linea completa durante l'esplorazione di Internet.

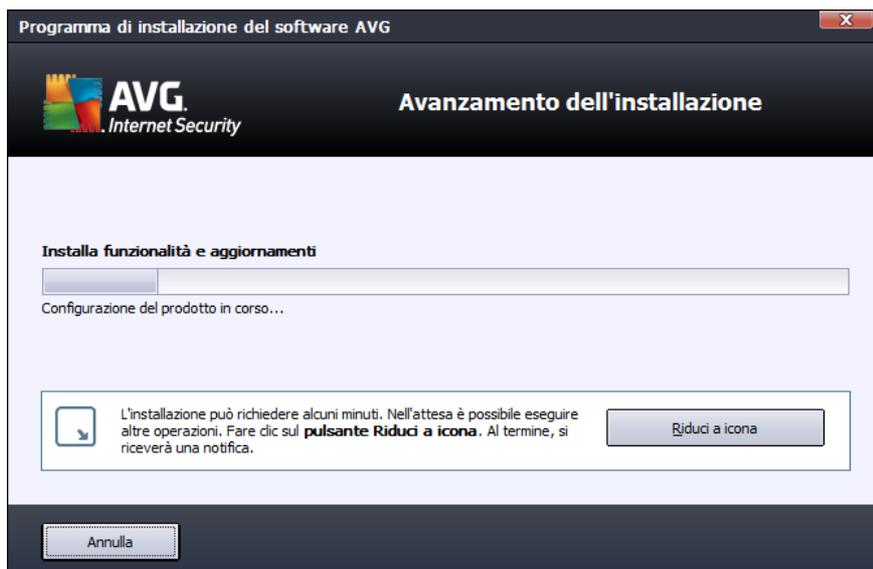
È inoltre possibile scegliere se utilizzare *AVG Secure Search (powered by Google)* come provider di ricerca predefinito. In caso affermativo, mantenere la relativa casella di controllo selezionata.

Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo di impostazione, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire subito dal processo di installazione. **AVG Internet Security 2012** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo di installazione.
- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo di installazione.

3.7. Avanzamento dell'installazione

Nella finestra di dialogo ***Avanzamento dell'installazione*** viene visualizzato l'avanzamento del processo di installazione. Non è necessario alcun intervento da parte dell'utente:

Al termine dell'installazione, si verrà reindirizzati automaticamente alla seguente finestra di dialogo.

Pulsanti di controllo

In questa finestra di dialogo è disponibile un solo pulsante di controllo: ***Annulla***. Questo pulsante deve essere utilizzato solo se si desidera arrestare il processo di installazione in corso. In tal caso **AVG Internet Security 2012** non verrà installato.

3.8. Installazione completata

La finestra di dialogo ***Installazione completata*** conferma che **AVG Internet Security 2012** è stato installato e configurato correttamente:

Programma di miglioramento del prodotto

Permette di decidere se partecipare al Programma di miglioramento del prodotto (*per dettagli, vedere il capitolo Impostazioni avanzate di AVG / Programma di miglioramento del prodotto*) che raccoglie informazioni anonime sulle minacce rilevate per aumentare il livello globale di protezione in Internet. In caso di accordo, mantenere l'opzione ***Accetto di partecipare al Programma di miglioramento del prodotto e della protezione Web di AVG 2012...*** selezionata *(l'opzione è attivata per impostazione predefinita)*.

Riavvio del computer

Per finalizzare il processo di installazione è necessario riavviare il computer: selezionare ***Riavvia subito*** per riavviare il computer immediatamente oppure ***Riavvia in seguito*** per posticipare l'operazione.

4. Dopo l'installazione

4.1. Registrazione del prodotto

Al termine dell'installazione di **AVG Internet Security 2012**, registrare il prodotto in linea nel sito Web di AVG (http://www.avg.com/). Dopo la registrazione sarà possibile ottenere l'accesso completo all'account utente AVG, alla newsletter di aggiornamento AVG e ad altri servizi offerti esclusivamente agli utenti registrati.

Il modo più facile per effettuare la registrazione è quello di procedere direttamente dall'interfaccia utente di **AVG Internet Security 2012**. Nel menu principale, selezionare la voce Guida in linea/ Registra ora. Si verrà reindirizzati alla pagine della ***registrazione*** del sito Web di AVG (http://www. avg.com/). Seguire le istruzioni fornite nella pagina.

4.2. Accesso all'interfaccia utente

È possibile accedere alla finestra di dialogo principale di AVG in diversi modi:

- tramite doppio clic sull'icona di AVG sulla barra delle applicazioni
- tramite doppio clic sull'icona di AVG sul desktop
- dal menu ***Start / Tutti i programmi / AVG 2012***

4.3. Scansione dell'intero computer

Esiste il rischio potenziale che un virus sia stato trasmesso al computer dell'utente prima dell'installazione di **AVG Internet Security 2012**. Per questo motivo è necessario eseguire Scansione intero computer per assicurarsi che non siano presenti infezioni sul PC. La prima scansione potrebbe richiedere diverso tempo *(circa un'ora)*, ma si consiglia di eseguirla comunque per verificare che il computer non sia stato compromesso da una minaccia. Per istruzioni sull'esecuzione di Scansione intero computer, consultare il capitolo Scansione AVG.

4.4. Controllo Eicar

Per confermare che **AVG Internet Security 2012** è stato installato correttamente è possibile eseguire il controllo EICAR.

Il controllo EICAR è un metodo standard e assolutamente sicuro per verificare il funzionamento del sistema antivirus. La sua esecuzione è sicura poiché non si tratta di un vero virus e non include frammenti di codice virale. La maggior parte dei prodotti vi reagisce come se si trattasse di un virus, *anche se normalmente lo segnala con un nome ovvio come "EICAR-AV-Test"*. È possibile scaricare il virus EICAR dal sito Web di EICAR all'indirizzo www.eicar.com, in cui si troveranno anche tutte le informazioni necessarie sul controllo EICAR.

Provare a scaricare il file ***eicar.com*** e a salvarlo sul disco locale. Subito dopo aver confermato il download del file di test, Online Shield (*parte del componente LinkScanner*) risponderà con un avviso. Questo avviso dimostra che AVG è stato installato correttamente nel computer.

Dal sito Web http://www.eicar.com è inoltre possibile scaricare la versione compressa del "virus" EICAR (*ad esempio nel formato eicar_com.zip*). Online Shield consente di scaricare questo file e di salvarlo sul disco locale, ma Resident Shield (*all'interno del componente Anti-Virus*) rileva il 'virus' quando si tenta di decomprimere il file.

Se AVG non identifica il file di controllo EICAR come un virus, è necessario verificare nuovamente la configurazione del programma.

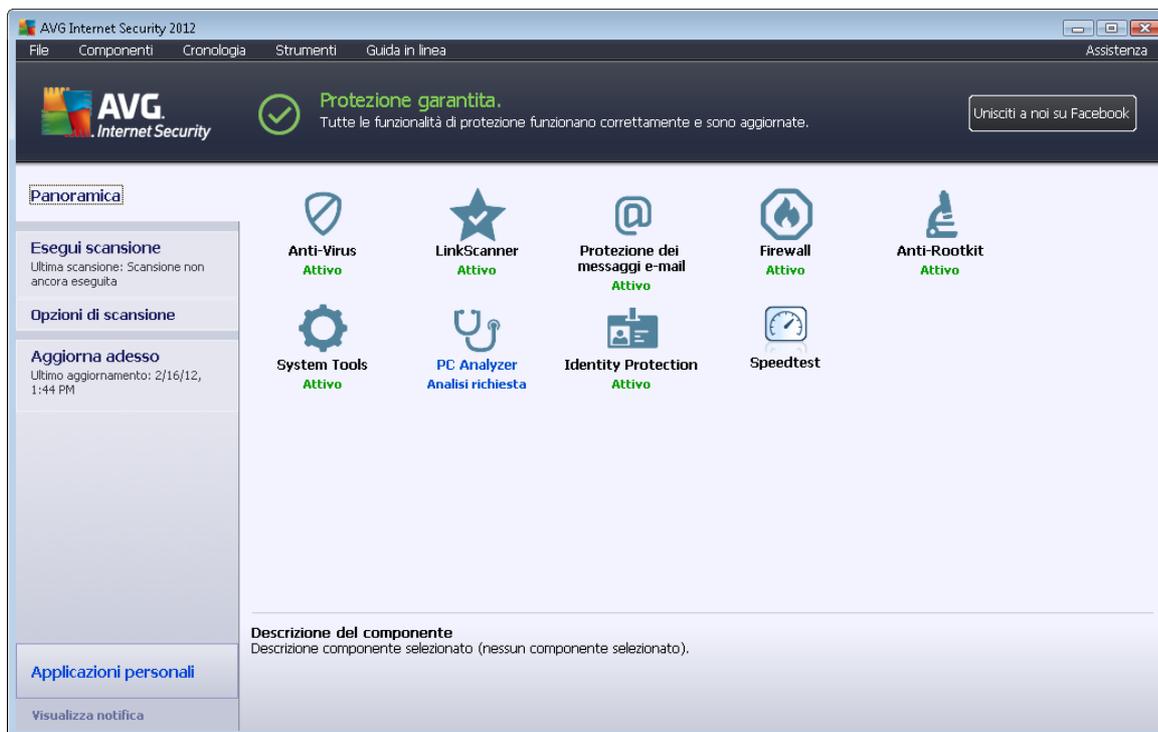
4.5. Configurazione predefinita di AVG

La configurazione predefinita (*ovvero la modalità di impostazione dell'applicazione dopo l'installazione*) di **AVG Internet Security 2012** è impostata dal fornitore del software in modo tale che tutti i componenti e le funzioni offrano un'ottimizzazione massima delle prestazioni.

A meno che non vi sia un motivo valido, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.

È possibile apportare alcune modifiche minori alle impostazioni dei componenti di AVG direttamente dall'interfaccia utente del componente specifico. Se è necessario cambiare la configurazione di AVG per adeguare l'applicazione alle proprie esigenze, accedere a Impostazioni AVG avanzate: selezionare la voce di menu ***Strumenti/Impostazioni avanzate*** e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.

5. Interfaccia utente di AVG

AVG Internet Security 2012 si apre visualizzando la finestra principale:

La finestra principale è suddivisa in diverse sezioni:

- ***Menu di sistema*** *(riga superiore nella finestra)* rappresenta l'esplorazione standard che consente di accedere a tutti i componenti, i servizi e le funzionalità di **AVG Internet Security 2012** – dettagli >>

- ***Informazioni sullo stato di protezione*** *(sezione superiore della finestra)* fornisce informazioni sullo stato corrente di **AVG Internet Security 2012** – dettagli >>

- Il pulsante ***Unisciti a noi su Facebook*** *(sezione superiore destra della finestra di dialogo)* consente di iscriversi alla community AVG su Facebook. Tuttavia, il pulsante viene visualizzato solo se tutti i componenti sono pienamente e correttamente funzionanti *(per ulteriori informazioni sullo stato dei componenti di AVG, vedere il capitolo Informazioni sullo stato di protezione)*

- ***Collegamenti rapidi*** *(sezione sinistra della finestra)* consentono di accedere rapidamente alle attività più importanti e più utilizzate di **AVG Internet Security 2012** – dettagli >>

- ***Applicazioni personali*** *(sezione inferiore sinistra della finestra)* apre una panoramica delle applicazioni aggiuntive disponibili per **AVG Internet Security 2012**: LiveKive, Family Safety e PC Tuneup

- ***Panoramica dei componenti*** *(sezione centrale della finestra)* offre una panoramica di tutti i componenti installati in **AVG Internet Security 2012** - dettagli >>

* ***Icona sulla barra delle applicazioni*** *(angolo inferiore destro del monitor, sulla barra delle applicazioni)* indica lo stato corrente di **AVG Internet Security 2012** - dettagli >>

* ***Gadget AVG*** *(sidebar di Windows, supportata in Windows Vista/7)* consente l'accesso rapido alle scansioni e agli aggiornamenti di **AVG Internet Security 2012** – dettagli >>

5.1. Menu di sistema

Menu di sistema è l'esplorazione standard utilizzata in tutte le applicazioni Windows. È posizionato orizzontalmente nella parte superiore della finestra principale di **AVG Internet Security 2012**. Utilizzare il menu di sistema per accedere a componenti, funzioni e servizi specifici di AVG.

Il menu di sistema è suddiviso in cinque sezioni principali:

5.1.1. File

* ***Esci***: consente di chiudere l'interfaccia utente di **AVG Internet Security 2012**. Tuttavia, l'applicazione AVG continuerà a essere eseguita in background e il computer sarà comunque protetto.

5.1.2. Componenti

Alla voce Componenti del menu di sistema sono disponibili i collegamenti a tutti i componenti AVG installati che consentono di aprire la rispettiva finestra di dialogo predefinita nell'interfaccia utente:

* ***Panoramica sistema***: consente di passare alla finestra di dialogo dell'interfaccia utente predefinita contenente una panoramica di tutti i componenti installati e del relativo stato

* ***Anti-Virus*** rileva virus, spyware, worm, trojan, librerie o file eseguibili indesiderati presenti nel sistema e protegge da adware dannoso - dettagli >>

* ***LinkScanner*** protegge dagli attacchi basati sul Web durante le ricerche e la navigazione in Internet – dettagli >>

* ***Protezione dei messaggi e-mail*** controlla la presenza di SPAM nei messaggi e-mail in entrata e blocca virus, attacchi di phishing o altre minacce – dettagli >>

* ***Firewall*** controlla tutte le comunicazioni su tutte le porte di rete, proteggendo il PC da attacchi pericolosi e bloccando tutti i tentativi di intrusione - dettagli >>

* ***Anti-Rootkit*** ricerca i rootkit pericolosi nascosti in applicazioni, driver o librerie – dettagli >>

* ***System Tools*** offre un riepilogo dettagliato dell'ambiente AVG e informazioni sul sistema operativo – dettagli >>

* ***PC Analyzer*** fornisce informazioni sullo stato del computer – dettagli >>

* ***Identity Protection*** protegge in modo costante le risorse digitali da minacce nuove e sconosciute – dettagli >>

* ***Amministrazione remota*** è disponibile solo nelle versioni AVG Business Edition se

durante il processo di installazione è stato richiesto di installare questo componente

5.1.3. Cronologia

- Risultati scansione: consente di visualizzare l'interfaccia di controllo di AVG, in particolare la finestra di dialogo Panoramica risultati di scansione

- Rilevamento Resident Shield: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da Resident Shield

- Rilevamento Scansione E-mail: consente di aprire una finestra di dialogo con una panoramica degli allegati e-mail rilevati come pericolosi dal componente Protezione dei messaggi e-mail

- Rilevamenti di Online Shield: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate dal servizio Online Shield incluso nel componente LinkScanner

- Quarantena virus: consente di aprire l'interfaccia dell'area di quarantena (Quarantena virus) in cui AVG sposta tutte le infezioni rilevate che per qualche motivo non è possibile eliminare automaticamente. All'interno della quarantena i file infetti sono isolati e la protezione del computer è garantita. Allo stesso tempo, i file infetti vengono archiviati per una possibile riparazione futura

- Log della Cronologia eventi: consente di aprire l'interfaccia della Cronologia eventi con una panoramica di tutte le azioni **AVG Internet Security 2012** registrate

- Log firewall: consente di aprire l'interfaccia delle impostazioni del Firewall nella scheda Log con una panoramica dettagliata di tutte le azioni del Firewall

5.1.4. Strumenti

- Scansione computer: avvia una scansione dell'intero computer.

- Scansione cartella selezionata...: consente di passare all'interfaccia di scansione di AVG e di definire i file e le cartelle da sottoporre a scansione nella struttura del computer.

- ***Scansione file...***: consente di eseguire un controllo su richiesta di un singolo file specifico. Fare clic su questa opzione per aprire una nuova finestra con la struttura del disco. Selezionare il file desiderato e confermare l'avvio della scansione.

- Aggiorna: avvia automaticamente il processo di aggiornamento di **AVG Internet Security 2012**.

- ***Aggiorna da directory...***: esegue il processo di aggiornamento dai file di aggiornamento che si trovano in una cartella specifica sul disco locale. Tuttavia, questa opzione è consigliabile solo in caso di emergenza, come situazioni in cui non si ottiene la connessione a Internet (*ad esempio, il computer è stato infettato e si è disconnesso da Internet, il computer è connesso a una rete senza accesso a Internet e così via*). Nella finestra appena aperta selezionare la cartella in cui è stato precedentemente posizionato il file di aggiornamento e avviare il processo di aggiornamento.

- Impostazioni avanzate...: apre la finestra di dialogo Impostazioni avanzate di AVG, in cui è

possibile modificare la configurazione di AVG Internet Security 2012. In genere è consigliabile mantenere le impostazioni dell'applicazione predefinite dal fornitore del software.

- Impostazioni Firewall...: apre una finestra di dialogo autonoma per la configurazione avanzata del componente Firewall.

5.1.5. Guida in linea

- ***Sommario***: consente di aprire i file della Guida di AVG
- ***Ottieni assistenza***: consente di aprire il sito Web di AVG (http://www.avg.com/) nella pagina del centro di assistenza clienti
- ***Web di AVG***: consente di aprire il sito Web di AVG (http://www.avg.com/)
- ***Informazioni sui virus e le minacce***: consente di aprire l'Enciclopedia dei virus in linea in cui è possibile trovare informazioni dettagliate sul virus identificato
- ***Riattiva***: consente di aprire la finestra di dialogo ***Attiva AVG*** con i dati immessi nella finestra di dialogo Personalizza AVG del processo di installazione. In questa finestra di dialogo è possibile immettere il numero di licenza per sostituire il numero di vendita (*il numero con cui è stata eseguita l'installazione di AVG*) o il numero di licenza in uso (*ad esempio, durante l'aggiornamento a un nuovo prodotto AVG*).
- ***Registra ora***: consente di aprire la pagina relativa alla registrazione del sito Web di AVG (http://www.avg.com/). Immettere i dati di registrazione. Solo i clienti che registrano il prodotto AVG possono ricevere assistenza tecnica gratuita.

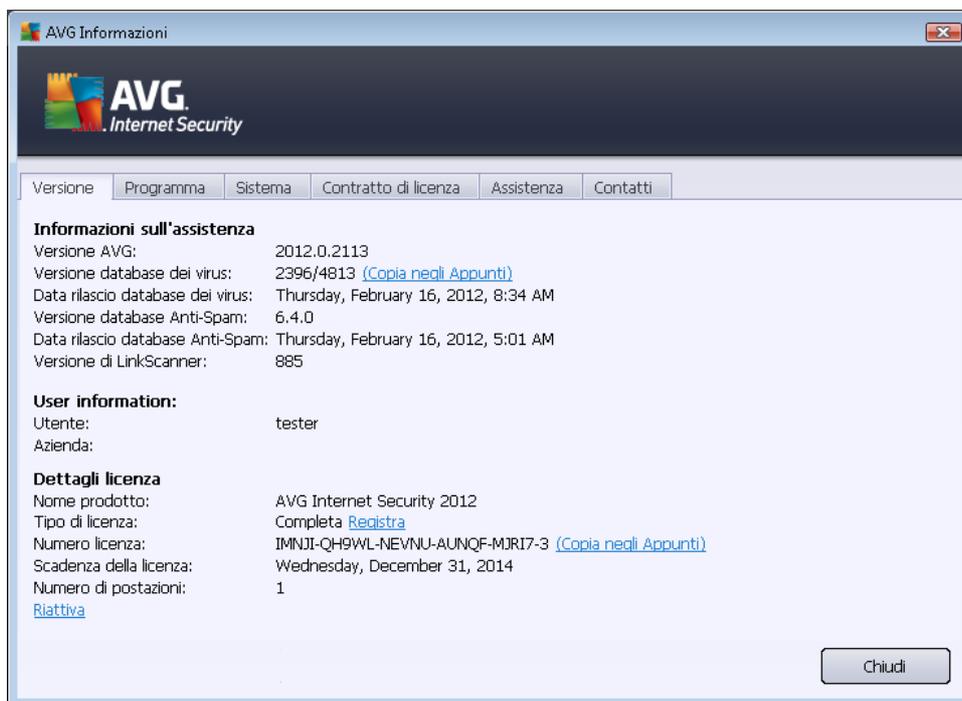
Nota*: se è in uso la versione Trial di* **AVG Internet Security 2012***, le ultime due voci appaiono come* ***Acquista ora*** *e* ***Attiva****, consentendo di acquistare subito la versione completa del programma. Per* **AVG Internet Security 2012** *installato con un numero di vendita, le voci vengono visualizzate come* ***Registra*** *e* ***Attiva****.*

- ***Informazioni su AVG***: consente di aprire la finestra di dialogo ***Informazioni***, che include sei schede in cui sono disponibili dati sul nome del programma, la versione del database dei virus e del programma, informazioni sul sistema, il contratto di licenza e le informazioni di contatto di ***AVG Technologies CZ***.

5.1.6. Assistenza

Il collegamento ***Assistenza*** apre una nuova finestra di dialogo denominata ***Informazioni*** che include tutti i tipi di informazioni necessarie quando si ricerca assistenza. La finestra di dialogo include dati di base sul programma AVG installato (*versione programma/database*), dettagli della licenza e un elenco di collegamenti rapidi per l'assistenza.

La finestra di dialogo ***Informazioni*** è suddivisa in sei schede:

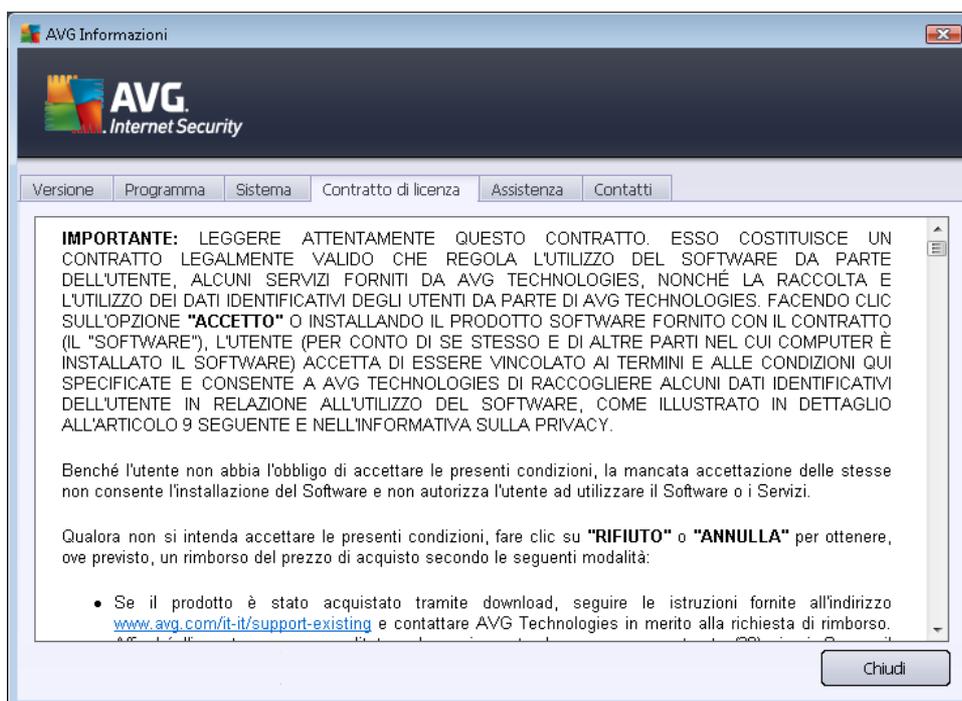
La scheda ***Versione*** è suddivisa in tre sezioni:

- ***Informazioni sull'assistenza***: fornisce informazioni sulla versione di **AVG Internet Security 2012**, sulla versione del database dei virus, sulla versione del database di Anti-Spam e sulla versione di LinkScanner .

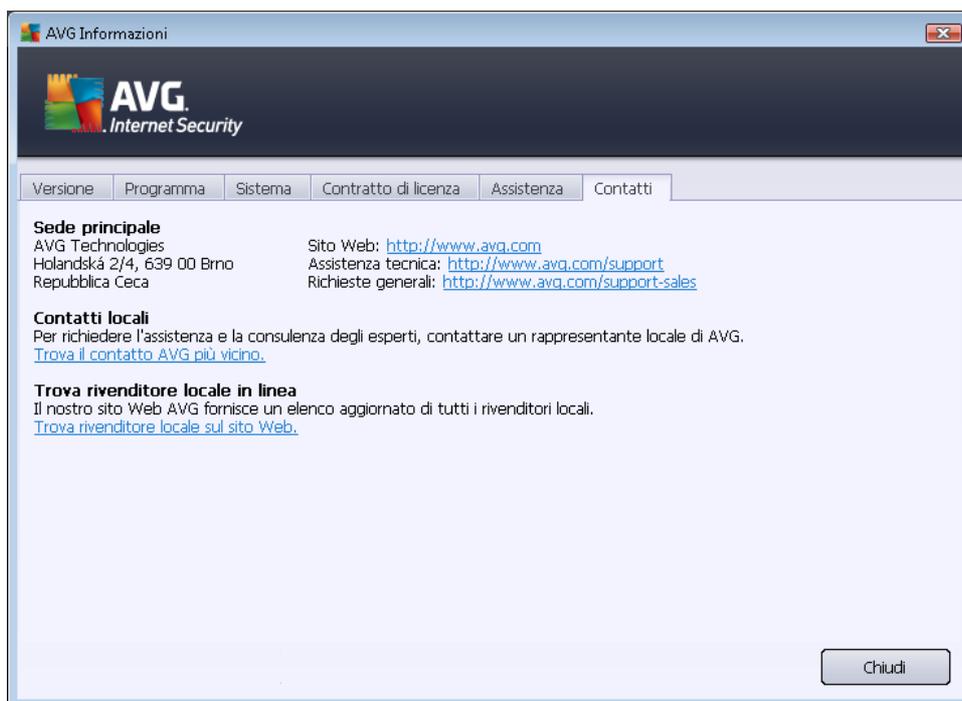
- ***Informazioni utente***: fornisce informazioni sull'utente e l'azienda titolari della licenza.

- ***Dettagli licenza***: fornisce informazioni sulla licenza *(nome del prodotto, tipo di licenza, numero di licenza, data di scadenza e numero di postazioni*). In questa sezione è inoltre possibile utilizzare il collegamento ***Registra*** per registrare **AVG Internet Security 2012** in linea; ciò consente di avvalersi completamente dell'assistenza tecnica AVG. Inoltre, utilizzare il collegamento ***Riattiva*** per aprire la finestra di dialogo ***Attiva AVG***. Immettere il numero di licenza nell'apposito campo per sostituire il numero di vendita *(che si utilizza durante l'installazione di AVG Internet Security 2012)* oppure per cambiare il numero di licenza corrente con un altro *(ad esempio quando si effettua l'upgrade a un prodotto AVG superiore)*.

Nella scheda ***Programma*** è possibile trovare informazioni sulla versione dei file di programma **AVG Internet Security 2012** e su codice di terzi utilizzato nel prodotto:

La scheda ***Sistema*** offre un elenco di parametri relativi al sistema operativo *(tipo di processore, sistema operativo e versione, numero di build, service pack utilizzati, memoria totale, memoria disponibile)*:

Nella scheda ***Contratto di licenza*** è disponibile il testo completo del Contratto di licenza tra l'utente e AVG Technologies:

La scheda ***Assistenza*** include un elenco di tutte le modalità di contatto dell'assistenza clienti. Inoltre, fornisce collegamenti al sito Web di AVG (http://www.avg.com/), ai forum AVG, alla sezione delle Domande frequenti e così via. Fornisce anche informazioni utili quando viene contattato il team dell'assistenza clienti:

La scheda ***Contatti*** fornisce un elenco di tutti i contatti di AVG Technologies, nonché dei contatti di rappresentanti e rivenditori AVG locali:

5.2. Informazioni sullo stato di protezione

La sezione ***Informazioni sullo stato di protezione*** si trova nella parte superiore della finestra principale di **AVG Internet Security 2012**. All'interno di questa sezione sono contenute le informazioni sullo stato di protezione corrente di **AVG Internet Security 2012**. Vedere la panoramica delle icone eventualmente visualizzate in questa sezione, con il relativo significato:

– L'icona verde indica che ***AVG Internet Security 2012 è correttamente funzionante***. Il computer è totalmente protetto, aggiornato e tutti i componenti installati funzionano correttamente.

– L'icona gialla indica ***la configurazione non corretta di uno o più componenti***. È consigliabile controllare le relative proprietà/impostazioni. Non sono presenti problemi gravi in **AVG Internet Security 2012** e probabilmente si è deciso di disattivare alcuni componenti per qualche ragione. La protezione è comunque attiva. Tuttavia, prestare attenzione alle impostazioni del componente in cui si sono verificati problemi. Il nome verrà fornito nella sezione ***Informazioni sullo stato di protezione***.

L'icona gialla viene inoltre visualizzata se, per qualche motivo, l'utente ha deciso di ignorare lo stato di errore di un componente. L'opzione ***Ignora stato del componente*** è disponibile nel

menu di scelta rapida *aperto tramite clic con il pulsante destro del mouse* sull'icona del rispettivo componente nella panoramica dei componenti della finestra principale di **AVG Internet Security 2012**. Selezionare questa opzione per confermare che si è al corrente dello stato di errore del componente, tuttavia si desidera mantenere **AVG Internet Security 2012** nella condizione attuale e non si desidera ricevere notifiche tramite l'icona presente nella barra delle applicazioni. Potrebbe essere necessario utilizzare ***Ignora stato del componente*** in situazioni particolari, tuttavia si consiglia di disattivare questa opzione nel più breve tempo possibile.

In alternativa, l'icona gialla verrà visualizzata anche se **AVG Internet Security 2012** richiede il riavvio del computer (***Riavvio necessario***). Prestare attenzione a questo avviso e riavviare il PC utilizzando il pulsante ***Riavvia ora*** .

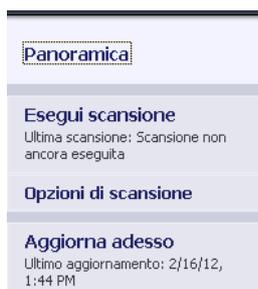
– L'icona arancione indica che ***AVG Internet Security 2012 si trova in uno stato critico.*** Uno o più componenti non funzionano correttamente e **AVG Internet Security 2012** non è in grado di proteggere il computer. Intervenire immediatamente per risolvere il problema segnalato. Se non si è in grado di correggere l'errore, contattare il team dell'Assistenza tecnica di AVG.

Se AVG Internet Security 2012 non è impostato per prestazioni ottimali, un nuovo pulsante denominato Correggi (oppure Correggi tutto se il problema riguarda più componenti) appare accanto alle informazioni sullo stato della protezione. Selezionare il pulsante per avviare un processo automatico di controllo e configurazione del programma. Questo è un modo rapido per impostare AVG Internet Security 2012 per prestazioni ottimali e ottenere il livello di protezione massimo.

Si consiglia di prestare attenzione alla sezione ***Informazioni sullo stato di protezione*** e, nel caso in cui fosse segnalato un problema, procedere cercando di risolverlo immediatamente. In caso contrario, il computer è a rischio.

Nota: *le informazioni sullo stato di AVG Internet Security 2012 sono inoltre sempre disponibili tramite l'icona sulla barra delle applicazioni.*

5.3. Collegamenti rapidi

I ***collegamenti rapidi*** si trovano nella parte sinistra dell'interfaccia utente di **AVG Internet Security 2012**. Questi collegamenti consentono di accedere immediatamente alle funzionalità più importanti e più utilizzate dell'applicazione, ossia scansione e aggiornamento. I collegamenti rapidi sono accessibili da tutte le finestre di dialogo dell'interfaccia utente:

I ***collegamenti rapidi*** sono suddivisi graficamente in tre sezioni:

- ***Esegui scansione***: per impostazione predefinita, il pulsante fornisce informazioni sull'ultima scansione avviata *(ossia tipo di scansione e data dell'ultimo avvio)*. Fare clic sul comando ***Esegui scansione*** per avviare di nuovo lo stesso tipo di scansione. Per avviare un altro tipo di scansione, fare clic sul collegamento ***Opzioni di scansione***. Viene aperta l'interfaccia di scansione di AVG in cui è possibile eseguire e pianificare scansioni o modificarne i parametri. *Per dettagli, vedere il capitolo Scansione AVG.*

- ***Opzioni di scansione***: utilizzare questo collegamento per passare da qualsiasi finestra di dialogo di AVG visualizzata alla finestra di dialogo predefinita, che contiene una panoramica di tutti i componenti installati. *Per dettagli, vedere il capitolo Panoramica dei componenti.*

- ***Aggiorna adesso***: il collegamento fornisce la data e l'ora dell'ultimo avvio dell' aggiornamento. Fare clic sul pulsante per eseguire subito il processo di aggiornamento e seguirne l'avanzamento. *Per dettagli, vedere il capitolo Aggiornamenti di AVG.*

I ***collegamenti rapidi*** sono accessibili dall'Interfaccia utente di AVG in qualsiasi momento. Una volta che si utilizza un collegamento rapido per eseguire un processo specifico, sia scansione che aggiornamento, l'applicazione visualizzerà una nuova finestra di dialogo, ma i collegamenti rimarranno comunque disponibili. Inoltre, il processo in esecuzione viene visualizzato graficamente nell'area di esplorazione, per offrire il controllo completo su tutti i processi in esecuzione all'interno di **AVG Internet Security 2012** in un dato momento.

5.4. Panoramica dei componenti

Sezione Panoramica dei componenti

La sezione ***Panoramica dei componenti*** si trova nella parte centrale dell'Interfaccia utente di **AVG Internet Security 2012**. La sezione è suddivisa in due parti:

- ***La panoramica di tutti i componenti installati*** che include un riquadro grafico per ciascun componente installato. Ciascun riquadro è identificato dall'icona del componente e fornisce informazioni sullo stato di attività o inattività corrente del rispettivo componente.

- ***La descrizione del componente*** che si trova nella parte inferiore della finestra di dialogo. La descrizione spiega brevemente la funzionalità di base del componente. Inoltre, fornisce informazioni sullo stato corrente del componente selezionato.

Elenco dei componenti installati

In **AVG Internet Security 2012** la sezione ***Panoramica dei componenti*** contiene informazioni sui seguenti componenti:

- ***Anti-Virus*** rileva virus, spyware, worm, trojan, librerie o file eseguibili indesiderati presenti nel sistema e protegge da adware dannoso - dettagli >>

- ***LinkScanner*** protegge da attacchi basati sul Web durante le ricerche e la navigazione in

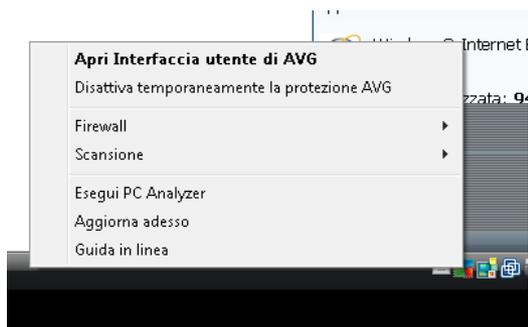
Internet – dettagli >>

- ***Protezione dei messaggi e-mail*** controlla la presenza di SPAM nei messaggi e-mail in entrata e blocca virus, attacchi di phishing o altre minacce – dettagli >>
- ***Firewall*** controlla tutte le comunicazioni su tutte le porte di rete, proteggendo il PC da attacchi pericolosi e bloccando tutti i tentativi di intrusione - dettagli >>
- ***Anti-Rootkit*** ricerca i rootkit pericolosi nascosti in applicazioni, driver o librerie – dettagli >>
- ***System Tools*** offre un riepilogo dettagliato dell'ambiente AVG e informazioni sul sistema operativo – dettagli >>
- ***PC Analyzer*** fornisce informazioni sullo stato del computer – dettagli >>
- ***Identity Protection*** protegge in modo costante le risorse digitali da minacce nuove e sconosciute – dettagli >>
- ***Amministrazione remota*** è disponibile solo nelle versioni AVG Business Edition se durante il processo di installazione è stato richiesto di installare questo componente

Azioni accessibili

- ***Posizionare il mouse sull'icona di un componente*** per evidenziarlo all'interno della panoramica dei componenti. Contemporaneamente, viene visualizzata la descrizione delle funzionalità di base del componente nella parte inferiore dell'interfaccia utente.
- ***Fare clic sull'icona di un componente*** per aprire l'interfaccia del componente con un elenco dei dati statistici di base.
- ***Fare clic con il pulsante destro del mouse sull'icona di un componente*** per espandere un menu di scelta rapida con diverse opzioni:
    - ***Apri***: fare clic su questa opzione per aprire la finestra di dialogo specifica del componente *(come avviene facendo clic sull'icona del componente)*.
    - ***Ignora stato del componente***: selezionare questa opzione per confermare che si è al corrente dello stato di errore del componente, tuttavia si desidera mantenere tale stato e non si desidera ricevere notifiche tramite l'icona presente nella barra delle applicazioni.
    - ***Apri nelle impostazioni avanzate...***: questa opzione è disponibile solo per alcuni componenti, ossia quelli che offrono la possibilità di regolare impostazioni avanzate.

5.5. Icona sulla barra delle applicazioni

L'***icona della barra delle applicazioni di AVG*** *(presente nella barra delle applicazioni di Windows, nell'angolo inferiore destro dello schermo)* indica lo stato corrente di **AVG Internet Security 2012**. È possibile visualizzarla in qualsiasi momento sulla barra delle applicazioni, indipendentemente dall'apertura o meno dell' interfaccia utente di **AVG Internet Security 2012**:

Aspetto dell'icona della barra delle applicazioni di AVG

- Se è completamente colorata e non presenta elementi aggiunti, l'icona indica che tutti i componenti di **AVG Internet Security 2012** sono attivi e funzionano correttamente. Tuttavia, l'icona può venire visualizzata in questo modo anche quando uno dei componenti non è completamente funzionante ma l'utente ha deciso di ignorare lo stato del componente . *Selezionando l'opzione Ignora stato del componente si conferma di essere al corrente dello stato di errore del componente, tuttavia si desidera mantenere la condizione attuale e non si desidera ricevere notifiche a riguardo.*

- L'icona con un punto esclamativo indica che un componente *o più componenti* si trovano in uno stato di errore. Prestare sempre attenzione a tale avviso e tentare di rimuovere il problema di configurazione del componente non impostato correttamente. Per modificare la configurazione del componente, fare doppio clic sull'icona della barra delle applicazioni per aprire l'interfaccia utente dell'applicazione. Per informazioni dettagliate sui componenti in stato di errore, consultare la sezione relativa alle informazioni sullo stato di protezione.

- L'icona della barra delle applicazioni può venire inoltre visualizzata completamente colorata con un fascio di luce rotante. Questa versione grafica segnala l'avvio di un processo di aggiornamento.

- La visualizzazione alternativa dell'icona completamente colorata con una freccia centrale indica che una scansione **AVG Internet Security 2012** è in esecuzione.

Informazioni sull'icona della barra delle applicazioni di AVG

L'***icona della barra delle applicazioni di AVG*** informa inoltre circa le attività correnti di **AVG Internet Security 2012** ed eventuali modifiche di stato del programma (*ad esempio avvio automatico di una scansione o un aggiornamento pianificato, attivazione dei profili Firewall, modifica*

dello stato di un componente, occorrenza di uno stato di errore e così via) tramite una finestra a comparsa che si apre sopra l'icona stessa:

Azioni accessibili tramite l'icona della barra delle applicazioni di AVG

L'***icona della barra delle applicazioni di AVG*** può inoltre essere utilizzata come collegamento rapido per accedere all'interfaccia utente di **AVG Internet Security 2012**, semplicemente tramite doppio clic. Se si fa clic con il pulsante destro del mouse sull'icona, viene aperto un menu di scelta rapida contenente le opzioni seguenti:

- ***Apri interfaccia utente di AVG***: fare clic per aprire l'interfaccia utente di **AVG Internet Security 2012**.
- ***Disattiva temporaneamente la protezione AVG***: questa opzione consente di disattivare completamente la protezione assicurata da **AVG Internet Security 2012**. Non utilizzare questa opzione se non è assolutamente necessario. Nella maggior parte dei casi, non è necessario disattivare **AVG Internet Security 2012** prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. Se fosse necessario disattivare temporaneamente **AVG Internet Security 2012**, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.
- ***Firewall***: fare clic per aprire il menu di scelta rapida delle opzioni di impostazione del Firewall in cui è possibile modificare i parametri principali: stato del Firewall (*firewall abilitato/firewall disabilitato/modalità di emergenza*), passaggio alla modalità gioco e profili Firewall.
- ***Scansioni***: fare clic per aprire il menu di scelta rapida delle scansioni predefinite (*Scansione intero computer* e *Scansione file o cartelle*) e selezionare la scansione richiesta, che verrà avviata immediatamente.
- ***Esecuzione delle scansioni in corso***: questa voce viene visualizzata solo se una scansione è in esecuzione sul computer. Per questa scansione è possibile impostare la priorità oppure arrestarla o sospenderla. Inoltre, sono accessibili le seguenti azioni: *Imposta priorità per tutte le scansioni, Sospendi tutte le scansioni* o *Arresta tutte le scansioni*.
- ***Esegui PC Analyzer***: fare clic per avviare il componente PC Analyzer.
- ***Aggiorna adesso***: viene avviato un aggiornamento immediato.
- ***Guida in linea***: apre il file della Guida alla pagina iniziale.

5.6. AVG Advisor

AVG Advisor è una funzionalità per le prestazioni che controlla continuamente tutti i processi in esecuzione nel PC in cerca di possibili problemi e che offre suggerimenti utili per evitare il problema. ***AVG Advisor*** è visualizzato sotto forma di una finestra popup che compare sulla barra delle applicazioni.

AVG Advisor potrebbe essere visualizzato nelle seguenti situazioni:

- Il browser Internet in uso sta esaurendo la memoria rallentando il lavoro *(AVG Advisor supporta solo i browser Internet Explorer, Chrome, Firefox, Opera e Safari).*
- Un processo in esecuzione nel computer sta consumando troppa memoria, rallentando le prestazioni del PC.
- Il computer sta per collegarsi automaticamente a una rete WiFi sconosciuta.

In tutti questi casi, ***AVG Advisor*** comunica la presenza di possibili problemi e fornisce il nome e l'icona del processo o dell'applicazione in conflitto. Inoltre, ***AVG Advisor*** suggerisce la procedura da eseguire per evitare i possibili problemi.

5.7. Gadget AVG

Il gadget AVG viene visualizzato sul desktop di Windows (*Windows Sidebar*). Questa applicazione è supportata solo sui sistemi operativi Windows Vista e Windows 7. ***Il gadget AVG*** offre l'accesso immediato alle funzionalità più importanti di **AVG Internet Security 2012**, ossia scansione e aggiornamento:

Accesso rapido a scansioni e aggiornamenti

Se necessario, il ***gadget AVG*** consente di avviare subito una scansione o un aggiornamento:

- ***Esegui scansione adesso***: fare clic sul collegamento ***Esegui scansione adesso*** per avviare direttamente la scansione dell'intero computer. È possibile visualizzare l'avanzamento del processo di scansione nell'interfaccia utente alternativa del gadget. Una breve panoramica delle statistiche fornisce informazioni sul numero di oggetti esaminati, minacce rilevate e minacce corrette. È possibile sospendere o arrestare il processo di scansione in corso in qualsiasi momento. Per dati dettagliati relativi ai risultati di scansione, consultare la finestra di dialogo standard Panoramica risultati di scansione che può essere aperta direttamente dal gadget tramite l'opzione ***Mostra dettagli*** *(i risultati di scansione pertinenti verranno elencati alla voce Scansione gadget sidebar)*.

- ***Aggiorna adesso***: fare clic sul collegamento ***Aggiorna adesso*AVG Internet Security 2012** per avviare l'aggiornamento direttamente dal gadget:

Accesso ai social network

Il gadget AVG fornisce inoltre un collegamento rapido per la connessione ai principali social network. Utilizzare il pulsante pertinente per accedere alle comunità AVG in Twitter, Facebook o LinkedIn:

- ***Collegamento Twitter*** : apre una nuova interfaccia del ***gadget AVG*** che fornisce una panoramica dei feed AVG più recenti pubblicati su Twitter. Seguire il collegamento ***Visualizza tutti i feed Twitter di AVG*** per aprire il browser Internet in una nuova finestra e passare direttamente al sito Web Twitter, in corrispondenza della pagina dedicata alle notizie relative a AVG:

- ***Collegamento Facebook*** : apre il browser Internet con il sito Web Facebook, in corrispondenza della pagina dedicata alla ***community AVG.***

- ***LinkedIn*** : questa opzione è disponibile solo nell'installazione di rete (*ovvero se AVG è stato installato utilizzando una licenza AVG Business Edition*) e apre il browser Internet in corrispondenza del sito Web ***AVG SMB Community*** all'interno del social network LinkedIn.

Altre funzionalità accessibili tramite il gadget

- ***PC Analyzer*** : apre l'interfaccia utente in corrispondenza del componente PC Analyzer e avvia subito l'analisi.

- ***Casella di ricerca***: digitare una parola chiave per ottenere subito i risultati della ricerca in una nuova finestra del browser Web predefinito.

6. Componenti di AVG

6.1. Anti-Virus

Il componente ***Anti-Virus*** è una pietra miliare di **AVG Internet Security 2012** e combina diverse funzioni fondamentali tipiche di un programma di protezione:

- Motore di scansione
- Protezione permanente
- Protezione anti-spyware

6.1.1. Motore di scansione

Il motore di scansione che costituisce la base del componente ***Anti-Virus*** esamina tutti i file e l'attività dei file *(apertura, chiusura e così via)* per ricercare virus noti. Tutti i virus rilevati verranno bloccati per essere poi corretti o messi in Quarantena virus.

La funzione importante della protezione AVG Internet Security 2012 è quella di bloccare l'esecuzione di tutti i virus noti.

Metodi di rilevamento

La maggior parte dei software antivirus utilizza anche la scansione euristica che consente di rilevare le caratteristiche tipiche dei virus, ossia le cosiddette firme virali. In questo modo la scansione antivirus è in grado di rilevare un nuovo virus sconosciuto, se il nuovo virus contiene alcune caratteristiche tipiche dei virus esistenti. L'***Anti-Virus*** utilizza i seguenti metodi di rilevamento:

- *Scansione*: ricerca di stringhe di caratteri specifiche di un determinato virus.
- *Analisi euristica*: emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale.
- *Rilevamento generale*: rilevamento di istruzioni caratteristiche del virus o del gruppo di virus specifico.

Se una sola tecnologia potrebbe avere esito negativo nel rilevamento o nell'identificazione di un virus, il componente ***Anti-Virus*** combina diverse tecnologie per assicurare che il computer sia protetto dai virus. **AVG Internet Security 2012** è anche in grado di analizzare e rilevare le applicazioni eseguibili o le librerie DLL che potrebbero essere potenzialmente indesiderate nel sistema. Queste minacce vengono denominate Programmi potenzialmente indesiderati *(vari tipi di spyware, adware e così via)*. Inoltre, **AVG Internet Security 2012** esegue la scansione del Registro di sistema alla ricerca di voci sospette, file Internet temporanei e cookie e consente di trattare tutti gli elementi potenzialmente dannosi come tutte le altre infezioni.

AVG Internet Security 2012 fornisce al computer la protezione continua.

6.1.2. Protezione permanente

AVG Internet Security 2012 offre la protezione continua sotto forma di protezione permanente. Il componente ***Anti-Virus*** esamina ogni singolo file *(con specifiche estensioni o senza estensioni)* aperto, salvato o copiato. Sorveglia le aree di sistema del computer e i supporti rimovibili (*dischi di memoria flash disk e così via*). Se viene rilevato un virus durante l'accesso a un file, arresta l'operazione in corso impedendo l'attivazione del virus. Normalmente, questo processo non viene notato dall'utente, poiché la protezione permanente funziona "in background". L'utente viene informato solo se vengono rilevate minacce; nel contempo, l'***Anti-Virus*** blocca l'attivazione della minaccia e la rimuove.

La protezione permanente viene caricata nella memoria del computer all'avvio ed è importante che resti sempre attiva.

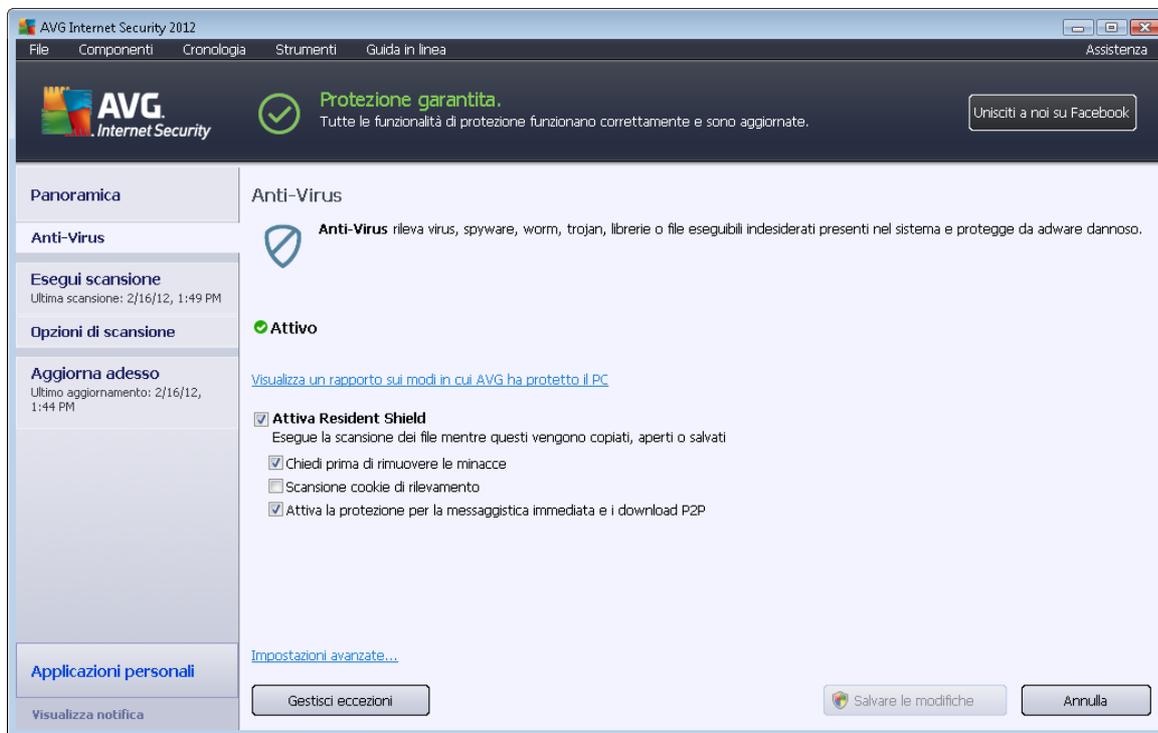
6.1.3. Protezione anti-spyware

Anti-Spyware include un database di spyware utilizzato per identificare i tipi di definizioni spyware noti. Gli esperti di AVG lavorano ininterrottamente per identificare e descrivere i più recenti schemi di spyware non appena questi emergono, quindi aggiungono le relative definizioni al database di spyware. Mediante il processo di aggiornamento, queste nuove definizioni vengono scaricate nel computer dell'utente al fine di proteggerlo in modo costante e affidabile, persino contro i tipi di spyware più recenti. ***Anti-Spyware*** consente di eseguire una scansione completa del computer alla ricerca di malware/spyware. È inoltre possibile rilevare malware inattivo, ovvero malware che è stato scaricato ma non ancora attivato.

Definizione di spyware

In genere per spyware si intende un particolare tipo di malware, ovvero un software che raccoglie informazioni dal computer senza informarne l'utente e senza richiederne l'autorizzazione. Alcune applicazioni spyware possono anche essere installate intenzionalmente e spesso contengono annunci pubblicitari, finestre popup o altri tipi di software indesiderato. Attualmente la fonte più comune di infezione sono i siti Web con contenuto potenzialmente pericoloso. Anche altri metodi di trasmissione, ad esempio i messaggi e-mail o le trasmissioni tramite worm e virus, sono molto diffusi. La protezione più importante consiste nell'utilizzo di un programma di scansione in background sempre attivo, ***Anti-Spyware***, che funziona come una protezione permanente ed esegue la scansione in background delle applicazioni mentre queste vengono eseguite.

6.1.4. Interfaccia dell'Anti-Virus

L'interfaccia del componente ***Anti-Virus*** fornisce una breve descrizione della funzionalità del componente, informazioni sullo stato corrente del componente *(Attivo)*, e opzioni di configurazione di base del componente:

Opzioni di configurazione

La finestra di dialogo fornisce alcune opzioni di configurazione di base delle funzioni disponibili nel componente ***Anti-Virus***. Viene fornita di seguito una breve descrizione di queste funzioni:

- ***Visualizza un rapporto in linea sui modi in cui AVG ha protetto il tuo PC***: il collegamento reindirizza a una pagina specifica del sito Web di AVG (http://www.avg.com/). In tale pagina è disponibile una panoramica statistica dettagliata di tutte le attività **AVG Internet Security 2012** eseguite sul computer in uno specifico periodo di tempo e in totale.

- ***Attiva Resident Shield***: questa opzione consente di attivare/disattivare rapidamente la protezione permanente. Resident Shield esegue la scansione dei file mentre questi vengono copiati, aperti o salvati. Se viene rilevato un virus o altra minaccia, l'utente ne viene avvisato immediatamente. Per impostazione predefinita la funzione è attivata e si consiglia di non modificare questa impostazione. Mediante la protezione permanente è possibile decidere come trattare le eventuali infezioni rilevate:

    - ***Chiedi prima di rimuovere le minacce***: mantenere l'opzione selezionata se si desidera che venga richiesta conferma ogni volta che una minaccia viene rilevata prima di essere spostata in Quarantena virus. La scelta non avrà alcun effetto sul livello di protezione, in quanto riflette esclusivamente le preferenze dell'utente.

    - ***Scansione cookie di rilevamento***: in modo indipendente dalle precedenti opzioni, è possibile decidere se effettuare la scansione per ricercare i cookie di rilevamento *(i cookie sono pacchetti di testo inviati da un server a un browser Web e inviati di nuovo intatti dal browser ogni volta che questo esegue l'accesso al server. I cookie*

HTTP sono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici). In casi specifici è possibile attivare questa opzione per ottenere livelli di massima protezione; tuttavia per impostazione predefinita l'opzione è disattivata.

  - ***Attiva la protezione per la messaggistica immediata e i download P2P***: selezionare questa voce se si desidera verificare che le comunicazioni di messaggistica immediata (*ad esempio ICQ, MSN Messenger e così via*) siano prive di virus.

- ***Impostazioni avanzate...***: fare clic sul collegamento per accedere alla relativa finestra di dialogo all'interno delle Impostazioni avanzate di **AVG Internet Security 2012**. In questa finestra di dialogo è possibile modificare la configurazione del componente nei dettagli. Tuttavia, tenere presente che la configurazione predefinita di tutti i componenti è stata impostata per far sì che **AVG Internet Security 2012** offra prestazioni ottimali e massima protezione. Si consiglia di mantenere la configurazione predefinita a meno che non siano presenti motivi validi per modificarla.

Pulsanti di controllo

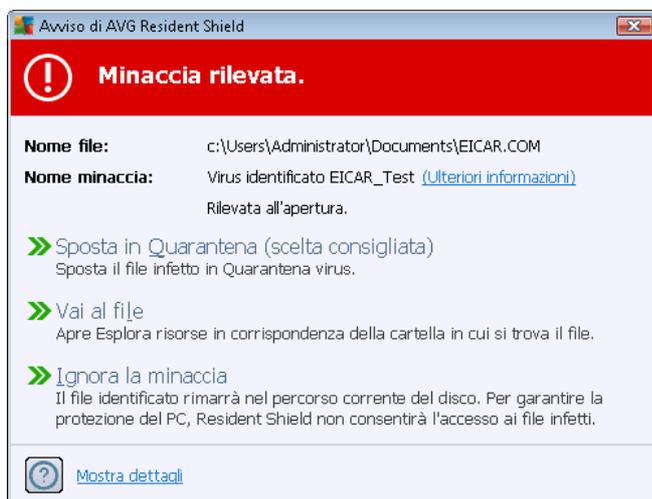
All'interno della finestra di dialogo è possibile utilizzare i seguenti pulsanti di controllo:

- ***Gestisci eccezioni***: consente di aprire una nuova finestra di dialogo denominata ***Resident Shield – Eccezioni***. La configurazione delle eccezionidalla scansione di Resident Shield è inoltre accessibile dal menu principale tramite Impostazioni avanzate / Anti-Virus / Resident Shield / Eccezioni *(consultare il relativo capitolo per una descrizione dettagliata)*. All'interno della finestra di dialogo è possibile specificare i file e le cartelle da escludere dalla scansione di Resident Shield. Se non è essenziale, si consiglia di non escludere alcun elemento. La finestra di dialogo fornisce i seguenti pulsanti di controllo:
  - *Aggiungi percorso*: consente di specificare una o più *directory* da escludere dalla scansione selezionandole una alla volta dalla struttura di esplorazione del disco locale.
  - *Aggiungi file*: consente di specificare i file da escludere dalla scansione selezionandoli uno alla volta dalla struttura di esplorazione del disco locale.
  - *Modifica elemento*: consente di modificare il percorso specificato di un file o una cartella selezionati.
  - *Rimuovi elemento*: consente di eliminare dall'elenco il percorso dell'elemento selezionato.
  - *Modifica elenco*: consente di modificare l'intero elenco delle eccezioni definite in una nuova finestra di dialogo utilizzabile come un editor di testo standard.
- ***Applica***: consente di salvare tutte le modifiche apportate alle impostazioni del componente in questa finestra di dialogo e di tornare all'interfaccia utente principale di **AVG Internet Security 2012** (*panoramica dei componenti*).

- ***Annulla***: consente di annullare tutte le modifiche apportate alle impostazioni del componente in questa finestra di dialogo. Non verrà salvata alcuna modifica. Verrà visualizzata di nuovo l'interfaccia utente principale di **AVG Internet Security 2012** (*panoramica dei componenti*).

6.1.5. Rilevamento Resident Shield

Minaccia rilevata!

Resident Shield esegue la scansione dei file mentre vengono copiati, aperti o salvati. Quando viene rilevato un virus o altra minaccia, l'utente viene avvisato immediatamente tramite la successiva finestra di dialogo:

In questa finestra di dialogo di avviso sono disponibili dati sul file rilevato e giudicato infetto (*Nome file*), il nome dell'infezione riconosciuta (*Nome minaccia*) e un collegamento all'Enciclopedia dei virus che include informazioni dettagliate sull'infezione rilevata, se nota (*Ulteriori informazioni*).

Quindi, è necessario decidere l'azione da intraprendere. Sono disponibili varie opzioni. ***Tenere presente che, in base a condizioni specifiche (tipo e posizione del file infetto), non tutte le opzioni sono sempre disponibili.***

- ***Correggi***: questo pulsante viene visualizzato solo se l'infezione rilevata può essere corretta. Quindi, il pulsante rimuove l'infezione dal file e ripristina il file allo stato originale. Se il file è un virus, utilizzare questa funzione per eliminarlo (*ossia spostarlo in Quarantena virus*)

- ***Sposta in Quarantena (consigliata)***: il virus verrà spostato in Quarantena virus

- ***Vai al file***: questa opzione reindirizza alla posizione esatta dell'oggetto sospetto (*apre una nuova finestra di Esplora risorse*)

- ***Ignora la minaccia***: si consiglia di NON utilizzare questa opzione a meno che non sussista un motivo valido per farlo.

Nota: *potrebbe accadere che le dimensioni dell'oggetto rilevato superino il limite di spazio libero in Quarantena virus. In tal caso, verrà visualizzato un avviso relativo al problema quando si tenterà di spostare l'oggetto infetto in Quarantena virus. Tuttavia, le dimensioni di Quarantena virus possono essere modificate. Tali dimensioni vengono definite come percentuale regolabile delle dimensioni effettive del disco rigido. Per aumentare le dimensioni di Quarantena virus, nella finestra di dialogo Quarantena virus, accessibile tramite Impostazioni AVG avanzate, è disponibile l'opzione Limite dimensione per Quarantena virus.*

Nella parte inferiore della finestra di dialogo è disponibile il collegamento ***Mostra dettagli***. Fare clic su di esso per aprire una finestra popup con informazioni dettagliate sul processo in esecuzione quando l'infezione è stata rilevata e i dati identificativi del processo.

Panoramica dei rilevamenti di Resident Shield

L'intera panoramica delle minacce rilevate da Resident Shield è disponibile nella finestra di dialogo ***Rilevamento Resident Shield*** accessibile tramite l'opzione del menu di sistema Cronologia / Rilevamento Resident Shield:

In ***Rilevamento Resident Shield*** è disponibile una panoramica di oggetti rilevati da Resident Shield, classificati come pericolosi e corretti o spostati in Quarantena virus. Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Infezione***: descrizione (eventualmente anche il nome) dell'oggetto rilevato
- ***Oggetto***: posizione dell'oggetto

- ***Risultato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui l'oggetto è stato rilevato
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati in alto. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***). Il pulsante ***Aggiorna elenco*** aggiorna l'elenco dei rilevamenti effettuati da ***Resident Shield***. Il pulsante ***Indietro*** consente di tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*).

6.2. LinkScanner

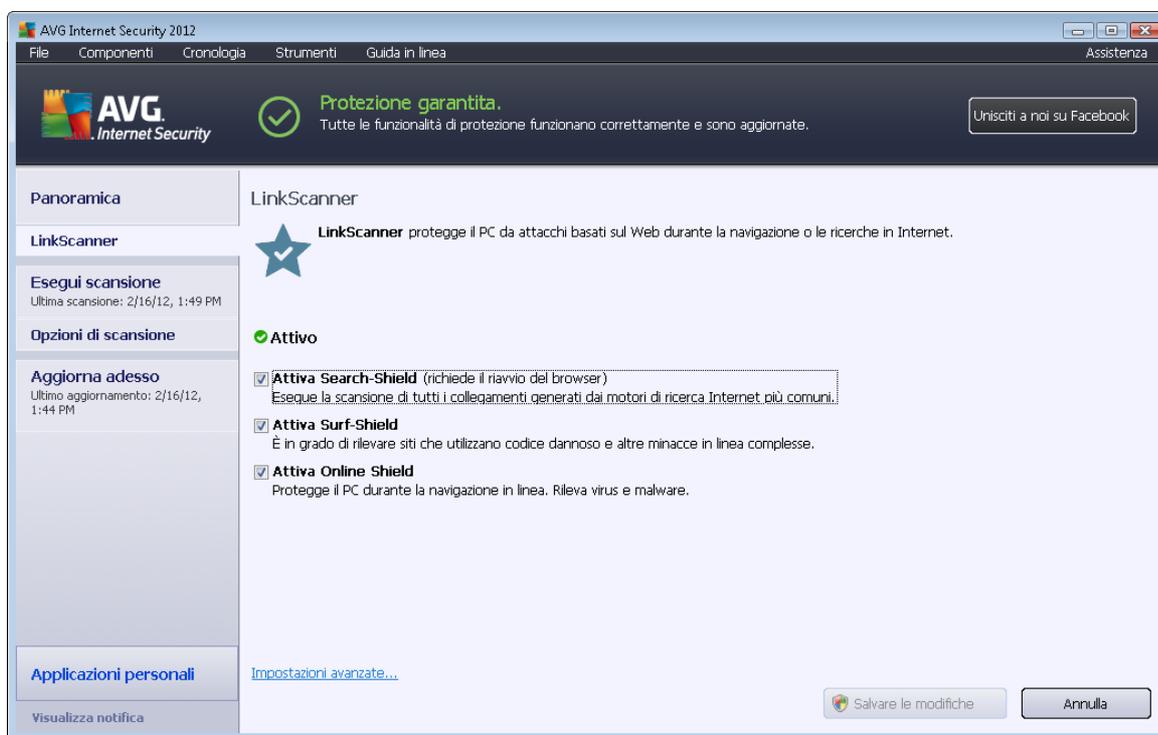
LinkScanner protegge dal numero sempre crescente di minacce transitorie presenti sul Web. Queste minacce possono nascondersi in qualsiasi tipo di sito Web, da quelli degli enti governativi, a quelli di grandi marchi famosi, a quelli di piccole aziende, e raramente restano in questi siti per più di 24 ore. ***LinkScanner*** protegge gli utenti analizzando le pagine Web dietro a tutti i collegamenti presenti sulla pagina Web visualizzata e garantendo che le pagine siano sicure nel momento cruciale, ovvero nell'attimo in cui si sta per fare clic sul collegamento.

Il componente LinkScanner non è destinato alla protezione delle piattaforme server.

La tecnologia ***LinkScanner*** include le seguenti funzionalità principali:

- Search-Shield contiene un elenco di siti Web *(indirizzi URL)* notoriamente pericolosi. Quando si effettuano ricerche con Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask e Seznam, tutti i risultati delle ricerche vengono controllati in base a questo elenco e viene visualizzata un'icona relativa al livello di sicurezza (*per Yahoo! vengono visualizzate solo le icone relative ai siti Web dannosi)*.
- Surf-Shield esegue la scansione dei contenuti dei siti Web visitati, indipendentemente dall'indirizzo del sito. Anche se un sito Web non viene rilevato da Search-Shield *(ad esempio quando viene creato un nuovo sito dannoso o quando un sito in precedenza sicuro contiene ora un malware)*, verrà rilevato e bloccato da Surf-Shield una volta che si tenterà di accedervi.
- Online Shield offre la protezione in tempo reale durante la navigazione in Internet. Esegue la scansione del contenuto delle pagine Web visitate (e dei possibili file in esse contenuti) persino prima che queste vengano visualizzate nel browser Web o scaricate nel computer. Online Shield rileva virus e spyware contenuti nella pagina che si sta per visitare arrestandone immediatamente il download per impedirne il trasferimento nel computer.
- ***AVG Accelerator*** ottimizza la riproduzione dei video in linea e semplifica il download. Quando il processo di accelerazione video è in corso, l'utente ne verrà informato tramite la finestra a comparsa sulla barra delle applicazioni.

6.2.1. Interfaccia di LinkScanner

La finestra di dialogo principale del componente LinkScanner fornisce una breve descrizione delle funzionalità del componente e informazioni sul relativo stato *(Attivo)*:

Nella parte inferiore della finestra di dialogo sono disponibili opzioni di configurazione di base per il componente:

- ***Attiva Search-Shield*** (*attivata per impostazione predefinita*): deselezionare la casella solo se esiste una motivazione valida per disattivare la funzionalità Search Shield.
- ***Attiva Surf-Shield*** (*attivata per impostazione predefinita*): protezione attiva (*in tempo reale*) da siti dannosi al momento dell'accesso. Le connessioni a siti dannosi noti e il loro contenuto vengono bloccati non appena l'utente esegue l'accesso mediante un browser Web (*o qualsiasi altra applicazione che utilizza HTTP*).
- ***Attiva Online Shield*** (*attivata per impostazione predefinita*): scansione in tempo reale delle pagine Web che si stanno per visitare alla ricerca di virus o spyware. Se vengono rilevate minacce, il download viene arrestato immediatamente in modo che queste non raggiungano il computer.

6.2.2. Rilevamenti di Search-Shield

Quando si eseguono ricerche in Internet con ***Search-Shield*** attivato, tutti i risultati di ricerca restituiti dai motori di ricerca più comuni (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg e SlashDot*) vengono controllati per rilevare l'eventuale presenza di collegamenti pericolosi o sospetti. Controllando i collegamenti e assegnando un contrassegno ai collegamenti dannosi, LinkScanner avvisa l'utente prima che faccia clic su collegamenti pericolosi o sospetti, in modo da garantire l'accesso solo ai siti Web sicuri.

Durante la valutazione di un collegamento nella pagina dei risultati della ricerca, verrà visualizzato un simbolo grafico vicino al collegamento per informare che la verifica è in corso. Una volta terminata la valutazione, verrà visualizzata la rispettiva icona informativa:

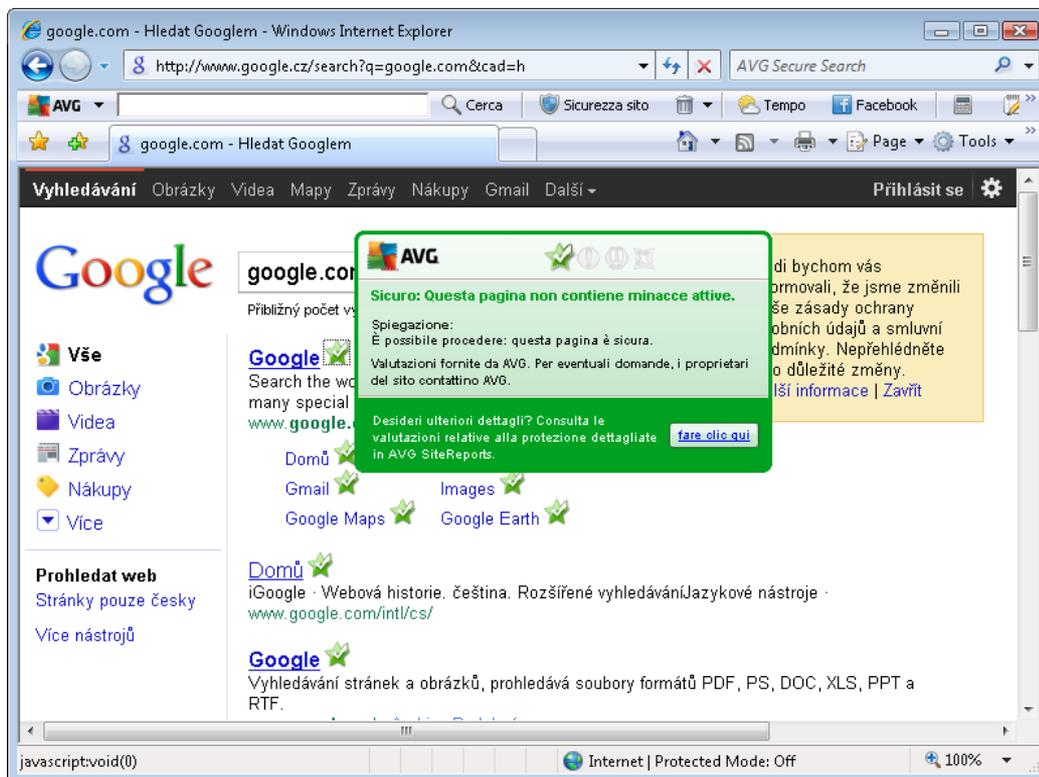
La pagina collegata è sicura.

La pagina alla quale fa riferimento il collegamento non contiene minacce ma risulta sospetta (*origine o motivazione dubbia, pertanto non è consigliabile utilizzarla per l'e-shopping e così via*).

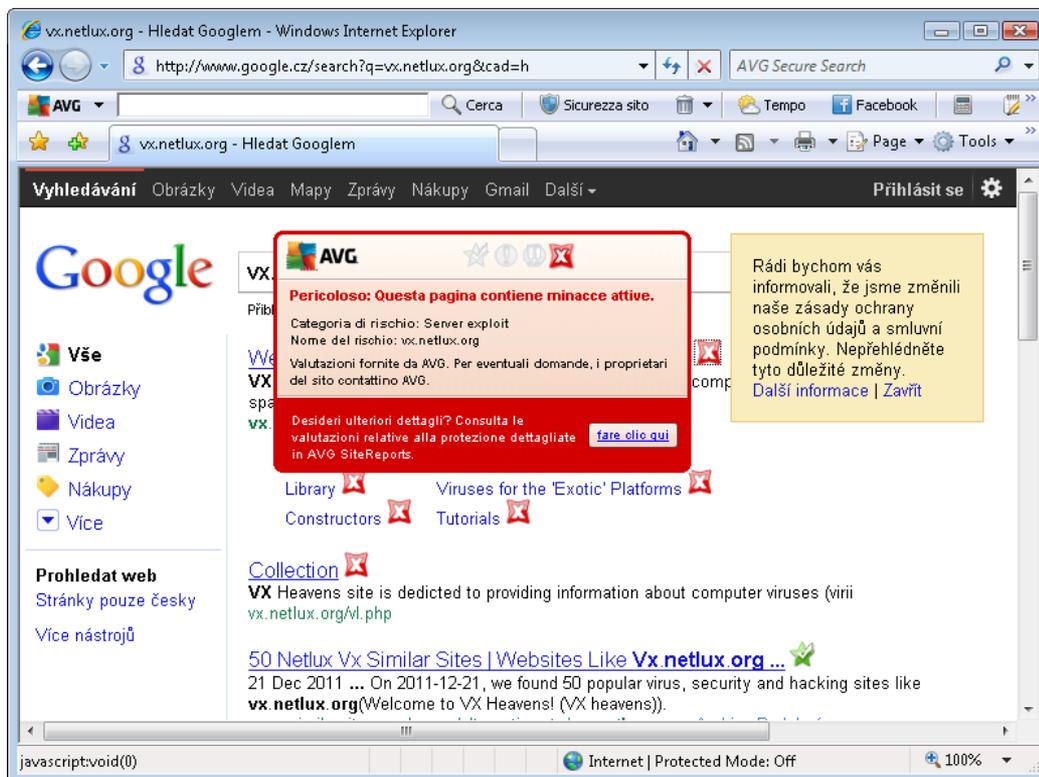
La pagina alla quale fa riferimento il collegamento potrebbe essere sicura, ma contenente a sua volta dei collegamenti a pagine decisamente pericolose, oppure la pagina potrebbe contenere del codice sospetto, anche se al momento non presenta minacce dirette.

La pagina collegata contiene minacce attive. Per motivi di sicurezza, non sarà consentito visitare questa pagina.

La pagina collegata non è accessibile, pertanto non è stato possibile eseguirne la scansione.

Se si passa il mouse sopra una singola icona che indica la valutazione verranno visualizzati i dettagli relativi al collegamento specifico. Le informazioni includono dettagli aggiuntivi relativi alla minaccia (*se presenti*):

6.2.3. Rilevamenti di Surf-Shield

Si tratta di un potente strumento di protezione che blocca il contenuto pericoloso delle pagine Web quando si tenta di aprirle, impedendone il download sul computer. Se questa funzionalità è abilitata, quando si fa clic sul collegamento o si digita l'URL di un sito pericoloso, l'apertura della pagina Web verrà bloccata immediatamente impedendo che il PC dell'utente venga infettato. È importante tenere presente che le pagine Web dannose possono infettare il computer con il semplice accesso al sito infetto. È per questo che quando si richiedono pagine Web contenenti exploit o altre gravi minacce, LinkScanner non ne consente la visualizzazione nel browser.

Se si incorre in siti Web dannosi, LinkScanner visualizzerà un avviso simile al seguente all'interno del browser:

L'accesso a questo sito Web è molto rischioso e non consigliabile.

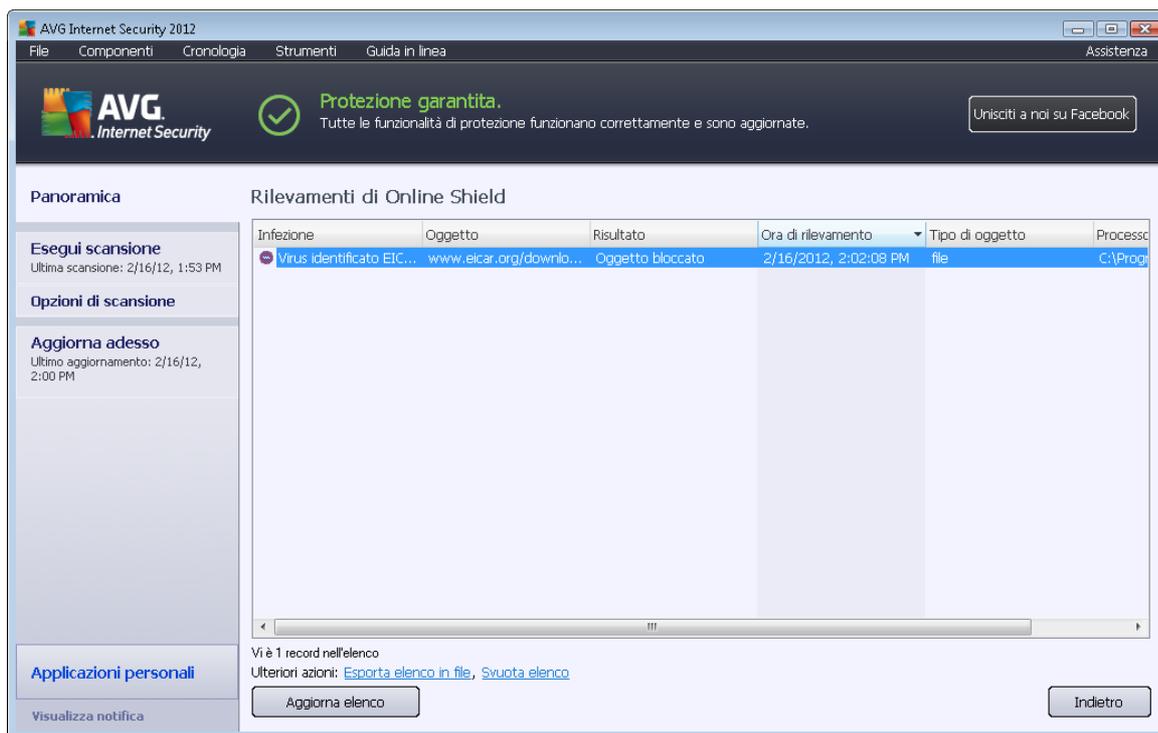
6.2.4. Rilevamenti di Online Shield

Online Shield esegue la scansione del contenuto delle pagine Web visitate e dei possibili file in esse contenuti prima che queste vengano visualizzate nel browser Web o scaricate nel computer. Se viene rilevata una minaccia, l'utente verrà avvisato immediatamente tramite la seguente finestra di dialogo:

In questa finestra di dialogo di avviso sono disponibili dati sul file rilevato e giudicato infetto (*Nome file*), il nome dell'infezione riconosciuta (*Nome minaccia*) e un collegamento all'Enciclopedia dei virus che include informazioni dettagliate sull'infezione rilevata (*se nota*). La finestra di dialogo fornisce i seguenti pulsanti:

- ***Mostra dettagli***: fare clic sul pulsante ***Mostra dettagli*** per aprire una finestra popup con informazioni sul processo in esecuzione quando l'infezione è stata rilevata e i dati identificativi del processo.

- ***Chiudi***: fare clic sul pulsante per chiudere la finestra di dialogo di avviso.

La pagina Web sospetta non verrà aperta e il rilevamento della minaccia verrà registrato nell'elenco ***Rilevamenti di Online Shield***; questa panoramica delle minacce rilevate è accessibile tramite il menu di sistema Cronologia / Rilevamenti di Online Shield.

Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Infezione***: descrizione *eventualmente anche il nome*) dell'oggetto rilevato
- ***Oggetto***: origine dell'oggetto (*pagina Web*)
- ***Risultato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui la minaccia è stata rilevata e bloccata
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati in alto. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***).

Pulsanti di controllo

- ***Aggiorna elenco***: aggiorna l'elenco dei rilevamenti effettuati da ***Online Shield***

- ***Indietro***: consente di tornare alla finestra di dialogo principale di AVG predefinita *(panoramica dei componenti)*

6.3. Protezione dei messaggi e-mail

Una delle origini più comuni di virus e trojan è l'e-mail. Phishing e spam rendono l'e-mail una fonte di rischio ancora più grande. Gli account e-mail gratuiti sono quelli che presentano più probabilità di ricevere questo tipo di messaggi dannosi, *poiché raramente impiegano una tecnologia antispam*, e gli utenti domestici si affidano moltissimo a questo tipo di e-mail. Inoltre, gli utenti domestici aumentano l'esposizione ad attacchi tramite e-mail poiché navigano spesso in siti sconosciuti e compilano moduli in linea con dati personali (*ad esempio l'indirizzo e-mail*). Di solito le società utilizzano account aziendali, filtri antispam e altri accorgimenti per ridurre il rischio.

Il componente ***Protezione dei messaggi e-mail*** è responsabile della scansione di tutti i messaggi e-mail, inviati o ricevuti; ogni volta che viene rilevato un virus in un'e-mail, questo viene immediatamente spostato in Quarantena virus. Il componente, inoltre, può filtrare alcuni tipi di allegati e-mail e aggiungere un testo di certificazione ai messaggi non infetti. ***Protezione dei messaggi e-mail*** include due funzioni principali:

- Scansione E-mail

- Anti-Spam

6.3.1. Scansione E-mail

Scansione e-mail personale esegue automaticamente la scansione delle e-mail in entrata e in uscita. È possibile utilizzarlo con i client e-mail che non dispongono di un plug-in in AVG (*ma può essere utilizzato anche per esaminare i messaggi e-mail per i client e-mail supportati da AVG con un plug-in specifico, ovvero Microsoft Outlook, The Bat e Mozilla Thunderbird*). Principalmente, è destinato all'uso con applicazioni e-mail quali Outlook Express, Incredimail e così via.

Durante l'installazione di AVG vengono creati due server per il controllo dell'e-mail: uno per il controllo delle e-mail in entrata e l'altro per il controllo delle e-mail in uscita. Grazie a questi due server, i messaggi e-mail vengono automaticamente controllati sulle porte 110 e 25 (*porte standard per l'invio e la ricezione dei messaggi*).

Scansione E-mail funziona come interfaccia tra il client e-mail e i server e-mail in Internet.

- ***Posta in entrata:*** quando viene ricevuto un messaggio dal server, il componente ***Scansione E-mail*** lo sottopone a scansione per il rilevamento di virus, rimuove gli allegati infetti e aggiunge la certificazione. Se rilevati, i virus vengono immediatamente inseriti in Quarantena virus. Quindi il messaggio viene passato al client e-mail.

- ***Posta in uscita:*** il messaggio viene inviato dal client e-mail a Scansione E-mail, che lo sottopone a scansione, insieme agli allegati, per il rilevamento di virus, quindi lo invia al server SMTP (*la scansione delle e-mail in uscita è disattivata per impostazione predefinita e può essere impostata manualmente*).

Il componente Scansione E-mail di non è destinato alle piattaforme server.

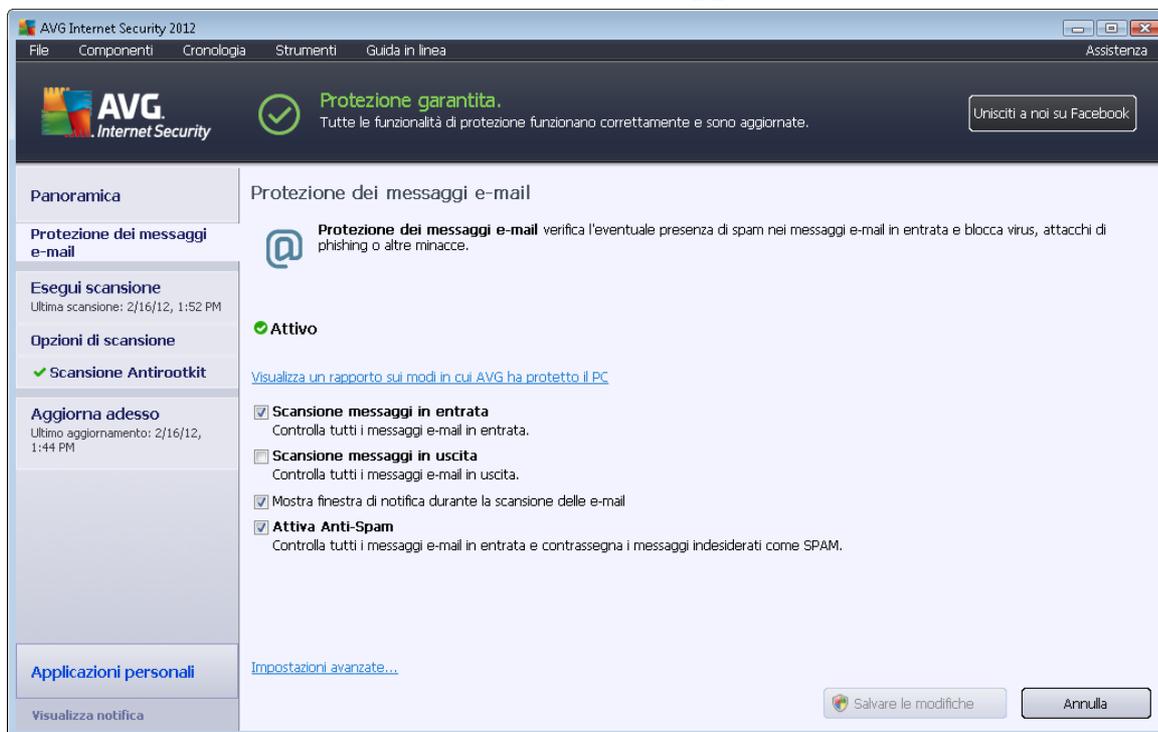
6.3.2. Anti-Spam

Come funziona l'Anti-Spam?

Anti-Spam controlla tutti i messaggi e-mail in entrata e contrassegna quelli indesiderati come spam. ***Anti-Spam*** può modificare l'oggetto dell'e-mail (*identificata come spam*) aggiungendo una stringa di testo speciale. Sarà quindi possibile filtrare rapidamente i messaggi e-mail nel client e-mail. ***Il componente Anti-Spam*** utilizza diversi metodi di analisi per elaborare ciascun messaggio e-mail, offrendo il massimo livello di protezione possibile contro i messaggi e-mail indesiderati. ***Anti-Spam*** utilizza un database aggiornato regolarmente per il rilevamento dello spam. È inoltre possibile utilizzare i server RBL (*database pubblici di indirizzi e-mail di spammer noti*) e aggiungere manualmente indirizzi e-mail alla whitelist (*indirizzi da non contrassegnare mai come spam*) e alla blacklist (*indirizzi da contrassegnare sempre come spam*).

Definizione di spam

Il termine "spam" indica messaggi di posta indesiderati, per lo più pubblicità di prodotti o servizi, inviati in massa e simultaneamente a un enorme numero di indirizzi di posta elettronica, che intasano le cassette postali dei destinatari. Lo spam non rientra nella categoria dei legittimi messaggi di posta elettronica commerciale per i quali i consumatori hanno fornito il loro consenso. Lo spam non è solo fastidioso ma può includere spesso anche truffe, virus o contenuti offensivi.

6.3.3. Interfaccia di Protezione dei messaggi e-mail

Nella finestra di dialogo ***Protezione dei messaggi e-mail*** è contenuto un breve testo che descrive la

funzionalità del componente e fornisce informazioni sul relativo stato corrente *(Attivo).* Utilizzare il collegamento ***Visualizza un rapporto in linea sui modi in cui AVG ha protetto il tuo PC*** per esaminare statistiche dettagliate di attività e rilevamenti di **AVG Internet Security 2012** in una pagina dedicata del sito Web di AVG (http://www.avg.com/).

Impostazioni di base di Protezione dei messaggi e-mail

Nella finestra di dialogo ***Protezione dei messaggi e-mail*** è possibile modificare ulteriormente alcune funzioni di base del componente:

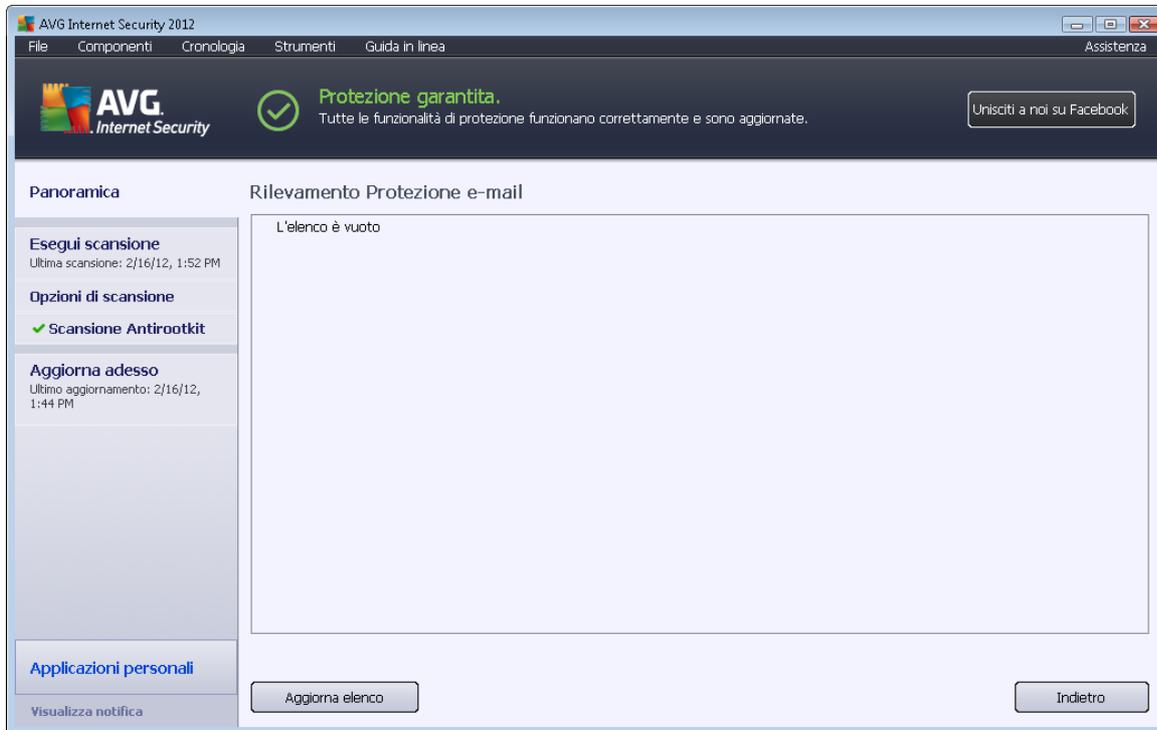
- ***Scansione messaggi in entrata*** *(attivata per impostazione predefinita)*: selezionare la casella di controllo per specificare che tutti i messaggi e-mail recapitati all'account devono essere sottoposti a scansione per il rilevamento di virus.
- ***Scansione messaggi in uscita*** *(disattivata per impostazione predefinita)*: selezionare la casella di controllo per specificare che tutti i messaggi e-mail inviati dall'account devono essere sottoposti a scansione per il rilevamento di virus.
- ***Visualizza finestra di notifica durante la scansione delle e-mail*** *(attivata per impostazione predefinita)*: selezionare la voce per confermare che si desidera essere informati tramite finestra di dialogo di notifica visualizzata sopra l'icona AVG presente nella barra delle applicazioni durante la scansione delle e-mail.
- ***Attiva Anti-Spam*** *(attivata per impostazione predefinita)*: selezionare la voce per specificare che si desidera che le e-mail indesiderate vengano filtrate dalla posta in arrivo.

Il fornitore del software ha impostato tutti i componenti di AVG per fornire prestazioni ottimali. A meno che non esista un motivo valido per farlo, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti. Se è necessario modificare la configurazione di AVG, selezionare la voce del menu di sistema Strumenti / Impostazioni avanzate e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.

Pulsanti di controllo

I pulsanti di controllo disponibili nella finestra di dialogo ***Protezione dei messaggi e-mail*** sono i seguenti:

- ***Salva modifiche***: selezionare questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo
- ***Annulla***: selezionare questo pulsante per tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*)

6.3.4. Rilevamenti di Scansione e-mail

Nella finestra di dialogo ***Rilevamento Scansione E-mail*** (*accessibile tramite l'opzione del menu di sistema Cronologia/Rilevamento Scansione E-mail*) sarà possibile visualizzare un elenco di tutti i rilevamenti effettuati dal componente Protezione dei messaggi e-mail. Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Infezione***: descrizione (eventualmente anche il nome) dell'oggetto rilevato
- ***Oggetto***: posizione dell'oggetto
- ***Risultato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui l'oggetto sospetto è stato rilevato
- ***Tipo di oggetto***: tipo di oggetto rilevato

Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati in alto. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***).

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di ***Rilevamento Scansione E-mail*** sono i seguenti:

- ***Aggiorna elenco***: aggiorna l'elenco delle minacce rilevate.
- ***Indietro***: torna alla finestra di dialogo visualizzata in precedenza.

6.4. Firewall

Il firewall è un sistema che impone un criterio di controllo dell'accesso tra due o più reti bloccando o consentendo il traffico. ***Il firewall*** contiene un insieme di regole che proteggono la rete interna da attacchi esterni *(normalmente provenienti da Internet)* e controlla tutte le comunicazioni su ogni singola porta di rete. La comunicazione viene valutata in base alle regole definite, quindi viene eventualmente consentita o impedita. Se il ***firewall*** rileva tentativi di intrusione, li blocca immediatamente e non consente all'intruso di accedere al PC.

Il firewall viene configurato per consentire o negare le comunicazioni interne/esterne (in entrambe le direzioni, entrata o uscita) tramite le porte definite e per le applicazioni software definite. Ad esempio, il firewall potrebbe essere configurato per consentire il solo flusso dei dati Web in entrata e in uscita tramite Microsoft Internet Explorer. Qualsiasi tentativo di trasmettere i dati Web tramite un altro browser viene quindi bloccato.

Il firewall impedisce l'invio non autorizzato delle informazioni di identificazione personale contenute nel computer. Controlla inoltre il modo in cui il computer scambia i dati con altri computer in Internet o nella rete locale. All'interno di un'organizzazione il ***firewall*** protegge anche i singoli computer da attacchi lanciati da utenti interni ai computer nella rete.

I computer non protetti da un firewall diventano un facile bersaglio per pirateria informatica e furti di dati.

Consiglio: *in genere non è consigliabile utilizzare più di un firewall su un singolo computer. Il livello di protezione del computer non è maggiore se si installano più firewall. È più probabile che si verifichino conflitti tra queste applicazioni. Si consiglia, pertanto, di utilizzare un solo firewall nel computer e di disattivare gli altri, eliminando così il rischio di possibili conflitti e problemi correlati.*

6.4.1. Principi del Firewall

In **AVG Internet Security 2012**, il ***Firewall*** controlla tutto il traffico su tutte le porte di rete del computer. In base alle regole definite, il componente ***Firewall*** valuta le applicazioni in esecuzione sul computer *(che vogliono eseguire la connessione alla rete locale o a Internet)* oppure le applicazioni che dall'esterno tentano di connettersi al PC dell'utente. Per ciascuna di queste applicazioni, il componente ***Firewall*** consente o impedisce la comunicazione sulle porte di rete. Per impostazione predefinita, se l'applicazione è sconosciuta *(ovvero non dispone di regole Firewall definite)*, il ***Firewall*** chiederà se si desidera consentire o bloccare il tentativo di comunicazione.

AVG Firewall non è destinato alle piattaforme server.

Funzionalità di AVG Firewall:

- Consente o blocca automaticamente tentativi di comunicazione di applicazioni note o chiede conferma
- Utilizza profili completi con regole predefinite, in base alle esigenze personali

- Attiva profili automaticamente durante la connessione a varie reti o durante l'utilizzo di diverse schede di rete

6.4.2. Profili Firewall

Il componente Firewall consente di definire regole di protezione specifiche a seconda del fatto che il computer in uso sia presente in un dominio, un computer autonomo o persino un notebook. Ogni opzione richiede un livello diverso di protezione e i livelli sono coperti dai rispettivi profili. In breve, un profilo di Firewall è una configurazione specifica del componente Firewall ed è possibile utilizzare diverse di queste configurazioni predefinite.

Profili disponibili

- ***Permetti Tutto***: è un profilo di sistema del componente Firewall predefinito dal produttore e sempre presente. Se questo profilo è attivato, tutte le comunicazioni di rete sono consentite e non vengono applicate regole dei criteri di protezione, come se la protezione del componente Firewall fosse disattivata (ossia tutte le applicazioni vengono contrassegnate come consentite ma i pacchetti continuano a essere controllati; per disattivare completamente i filtri è necessario disattivare il componente Firewall). Questo profilo di sistema non può essere duplicato o eliminato e le relative impostazioni non possono essere modificate.

- ***Blocca Tutto***: è un profilo di sistema del componente Firewall predefinito dal produttore e sempre presente. Quando il profilo è attivato, tutte le comunicazioni di rete sono bloccate e non è possibile accedere al computer da reti esterne né comunicare con l'esterno. Questo profilo di sistema non può essere duplicato o eliminato e le relative impostazioni non possono essere modificate.

- ***Profili personalizzati***: i profili personalizzati consentono di avvalersi della funzionalità di attivazione automatica del profilo, particolarmente utile se si effettua frequentemente la connessione a varie reti *(ad esempio con un notebook).* I profili personalizzati vengono generati automaticamente dopo l'installazione di **AVG Internet Security 2012** e coprono le singole esigenze delle regole dei criteri del Firewall. Sono disponibili i seguenti profili personalizzati:

  - ***Direttamente connesso a Internet***: adatto ai PC o ai notebook comuni connessi direttamente a Internet, senza alcuna protezione aggiuntiva. Questa opzione è inoltre consigliata se il notebook viene connesso a varie reti sconosciute e probabilmente non protette (*ad esempio in Internet point, stanze di albergo e così via.*). Le regole dei criteri del Firewall più rigide di questo profilo garantiscono che il computer sia adeguatamente protetto.

  - ***Computer in dominio***: adatta per computer in una rete locale, in genere a scuola o in ufficio. Si presume che la rete abbia un amministratore e sia protetta tramite misure aggiuntive per cui il livello di protezione può essere più basso rispetto a quello dei casi precedenti per consentire l'accesso a cartelle e unità disco condivise e così via.

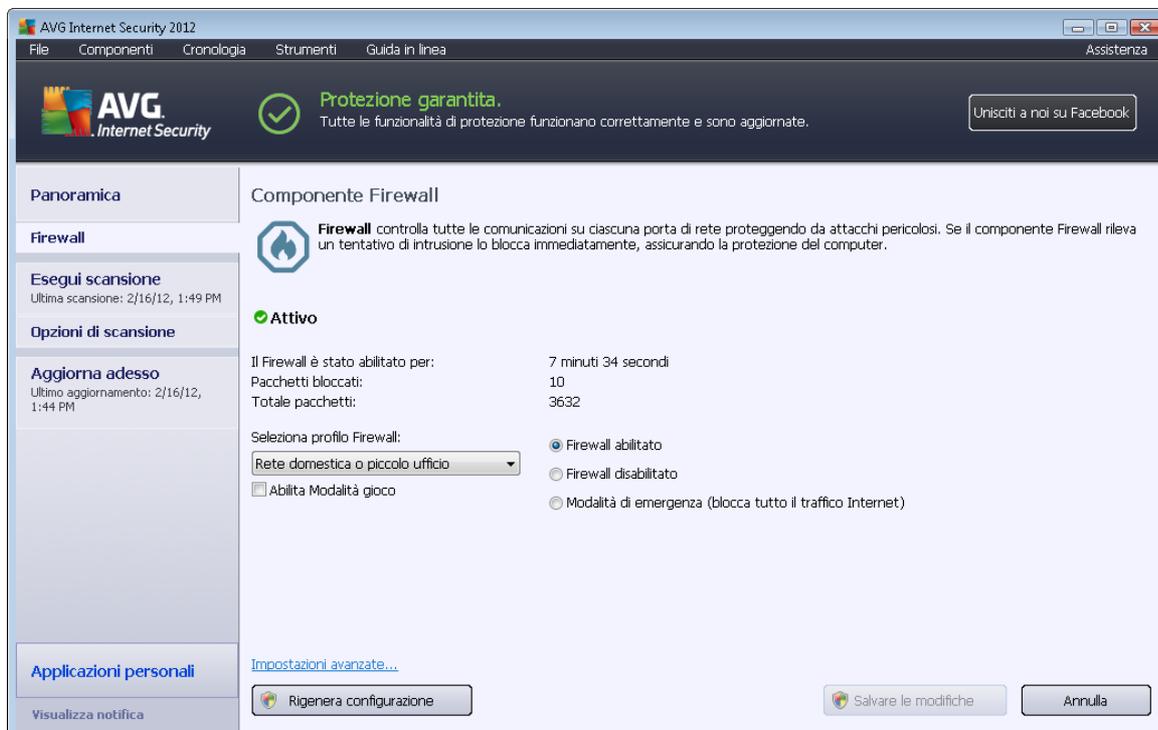
  - ***Rete domestica o piccolo ufficio***: adatta per computer in una piccola rete, in genere a casa o in una piccola azienda. In genere, questo tipo di rete non ha un

amministratore "centrale" ed è semplicemente costituita da diversi computer connessi tra loro che condividono una stampante, uno scanner o un altro dispositivo simile, che le regole del Firewall devono considerare.

Attivazione profili

La funzionalità di attivazione dei profili consente di attivare automaticamente il componente Firewall in base al profilo definito quando si utilizza una determinata scheda di rete o quando viene eseguita la connessione a un determinato tipo di rete. Se non sono ancora stati assegnati profili a un'area di rete, alla successiva connessione a quest'area il componente Firewall visualizzerà una finestra di dialogo in cui verrà richiesta l'assegnazione di un profilo. È possibile assegnare profili a tutte le aree o interfacce di rete locali e specificare ulteriori impostazioni nella finestra di dialogo Profili di aree e schede, in cui è possibile anche disabilitare la funzionalità se non si desidera utilizzarla (*quindi, per qualsiasi tipo di connessione, verrà utilizzato il profilo predefinito*).

Di norma, gli utenti che dispongono di un notebook e utilizzano vari tipi di connessione riterranno molto utile questa funzionalità. Se si dispone di un computer desktop e si utilizza sempre un solo tipo di connessione (*ad esempio, connessione via cavo a Internet*), non dovrebbero esserci problemi di attivazione dei profili, in quanto probabilmente non verranno mai utilizzati.

6.4.3. Interfaccia del Firewall

La finestra di dialogo principale ***Componente Firewall*** fornisce informazioni di base sulla funzionalità del componente e il relativo stato *(Attivo)*, nonché una breve panoramica delle statistiche del componente:

- ***Il firewall è stato abilitato per***: tempo trascorso dall'ultimo avvio del firewall
- ***Pacchetti bloccati***: numero di pacchetti bloccati rispetto all'intera quantità di pacchetti controllati
- ***Totale pacchetti***: numero di tutti i pacchetti controllati durante l'esecuzione del firewall

Impostazioni Firewall di base

- ***Seleziona profilo Firewall***: dal menu a discesa selezionare uno dei profili definiti (*per una descrizione dettagliata di ciascun profilo e il relativo uso consigliato, consultare il capitolo Profili Firewall*)
- ***Abilita modalità gioco***: selezionare questa opzione per assicurare che, durante l'esecuzione di applicazioni a schermo intero (*giochi, presentazioni, film e così via*), il Firewall non visualizzi finestre di dialogo per richiedere se consentire o bloccare la comunicazione per applicazioni sconosciute. Se un'applicazione sconosciuta tenta di comunicare sulla rete in quel momento, il Firewall consente o blocca automaticamente il tentativo in base alle impostazioni presenti nel profilo corrente. ***Nota:*** se la modalità gioco è attivata, tutte le attività pianificate (scansioni e aggiornamenti) vengono posticipate finché l'applicazione non viene chiusa.
- Inoltre, nella sezione delle impostazioni di base è possibile selezionare tre opzioni alternative che definiscono lo stato corrente del componente Firewall:
  - ***Firewall abilitato*** *(impostazione predefinita)*: selezionare questa opzione per consentire la comunicazione alle applicazioni contrassegnate come 'consentite' nell'insieme di regole definito all'interno del profilo Firewall selezionato.
  - ***Firewall disabilitato***: questa opzione consente di disattivare completamente il componente Firewall. Tutto il traffico di rete viene consentito ma non controllato.
  - ***Modalità di emergenza (blocca tutto il traffico Internet)***: selezionare questa opzione per bloccare tutto il traffico su ogni singola porta di rete; il Firewall è ancora in esecuzione ma tutto il traffico di rete viene interrotto.

Nota: *il produttore del software ha impostato tutti i componenti di AVG Internet Security 2012 per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti. Se è necessario modificare la configurazione del Firewall, selezionare la voce di menu di sistema* ***Strumenti / Impostazioni Firewall*** *e modificare la configurazione del Firewall nella finestra di dialogo Impostazioni Firewall visualizzata.*

Pulsanti di controllo

- ***Rigenera configurazione***: selezionare questo pulsante per sovrascrivere la configurazione corrente del Firewall e ripristinare la configurazione predefinita basata sul rilevamento automatico.

- ***Salva modifiche***: selezionare questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo.

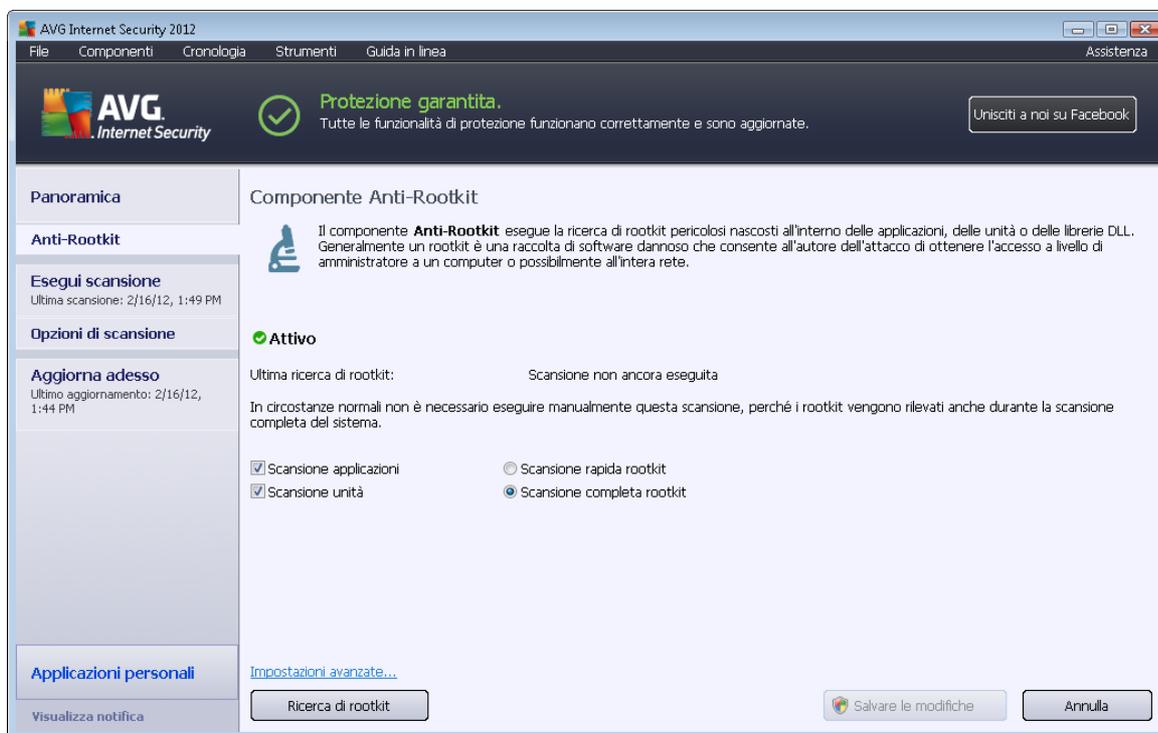
- ***Annulla***: selezionare questo pulsante per tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*).

6.5. Anti-Rootkit

Anti-Rootkit è uno strumento specializzato per il rilevamento e la rimozione efficace di rootkit dannosi, ossia programmi e tecnologie che possono camuffare la presenza di software dannoso sul computer. ***Anti-Rootkit*** è in grado di rilevare i rootkit in base a un gruppo di regole predefinito. Tenere presente che vengono rilevati tutti i rootkit *(non solo quelli infetti)*. Se ***Anti-Rootkit*** rileva un rootkit, ciò non significa necessariamente che il rootkit sia infetto. Talvolta i rootkit vengono utilizzati come driver o fanno parte di applicazioni regolari.

Definizione di rootkit

Un rootkit è un programma progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. L'accesso all'hardware è raramente necessario poiché un rootkit dovrà assumere il controllo del sistema operativo in esecuzione sull'hardware. In genere, i rootkit agiscono per nascondere la propria presenza sul sistema tramite sovversione o espedienti relativi ai meccanismi di protezione standard del sistema operativo. Si tratta spesso anche di trojan che ingannano gli utenti facendo loro credere di poter essere eseguiti in tutta sicurezza sui sistemi. Le tecniche utilizzate a questo scopo possono includere l'occultamento di processi in esecuzione dai programmi di monitoraggio oppure di file o dati di sistema dal sistema operativo.

6.5.1. Interfaccia dell'Anti-Rootkit

La finestra di dialogo ***Anti-Rootkit*** fornisce una breve descrizione della funzionalità del componente, segnala lo stato corrente del componente*(Attivo)* e indica l'ultimo avvio del controllo ***Anti-Rootkit*** (*Ultima ricerca di rootkit; il test anti-rootkit è un processo predefinito eseguito nell'ambito della Scansione intero computer*). La finestra di dialogo ***Anti-Rootkit*** fornisce inoltre il collegamento a Strumenti/Impostazioni avanzate. Utilizzare il collegamento per passare all'ambiente di configurazione avanzata del componente ***Anti-Rootkit***.

Il fornitore del software ha impostato tutti i componenti di AVG per fornire prestazioni ottimali. A meno che non vi sia un motivo valido, si consiglia di non modificare la configurazione di AVG. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.

Impostazioni Anti-Rootkit di base

Nella parte inferiore della finestra di dialogo è possibile impostare funzioni di base della scansione anti-rootkit. Selezionare innanzitutto le caselle di controllo corrispondenti per specificare gli oggetti da sottoporre a scansione:

- ***Scansione applicazioni***
- ***Scansione unità***

Quindi, è possibile selezionare la modalità di scansione anti-rootkit:

- ***Scansione rapida rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*).
- ***Scansione completa rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*), nonché tutte le unità locali (*inclusa l'unità di memoria flash, ma escluse le unità disco floppy/CD*).

Pulsanti di controllo

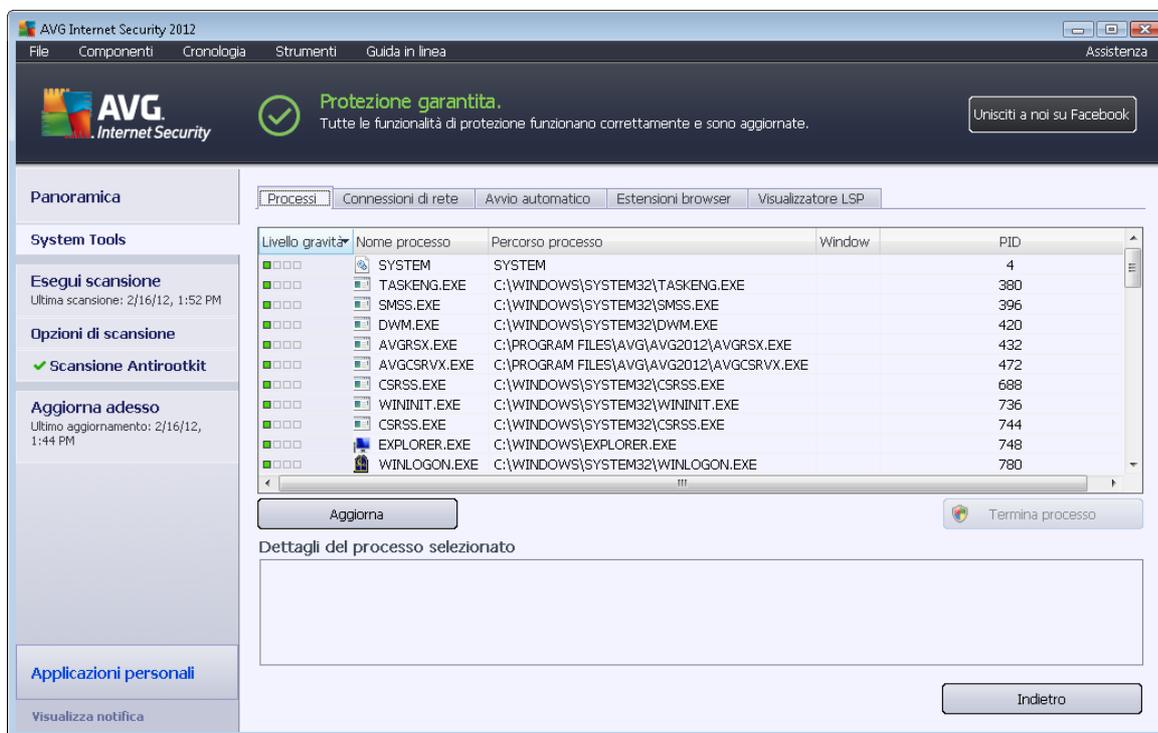
- ***Ricerca di rootkit***: poiché la scansione anti-rootkit non è inclusa nella Scansione intero computer, è possibile eseguire la scansione anti-rootkit direttamente dall'interfaccia dell' ***Anti-Rootkit*** utilizzando questo pulsante.
- ***Salva modifiche***: selezionare questo pulsante per salvare tutte le modifiche apportate in questa interfaccia e tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*).
- ***Annulla***: selezionare questo pulsante per tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*) senza salvare le modifiche apportate.

6.6. System Tools

System Tools si riferisce a strumenti che offrono un riepilogo dettagliato dell'ambiente **AVG Internet Security 2012** e del sistema operativo. Il componente visualizza una panoramica degli elementi seguenti:

- Processi: elenco dei processi (*ossia le applicazioni in esecuzione*) attivi nel computer
- Connessioni di rete: elenco delle connessioni attive
- Avvio automatico: elenco di tutte le applicazioni eseguite durante l'avvio del sistema Windows
- Estensioni browser: elenco dei plug-in (*ossia le applicazioni*) installate nel browser Internet
- Visualizzatore LSP: elenco dei Layered Service Provider (*LSP*)

È anche possibile modificare panoramiche specifiche, ma questa operazione è consigliabile solo a utenti molto esperti.

6.6.1. Processi

Nella finestra di dialogo ***Processi*** è incluso un elenco di processi (*ad esempio, applicazioni in esecuzione*) attualmente attivi sul computer. L'elenco è suddiviso in varie colonne:

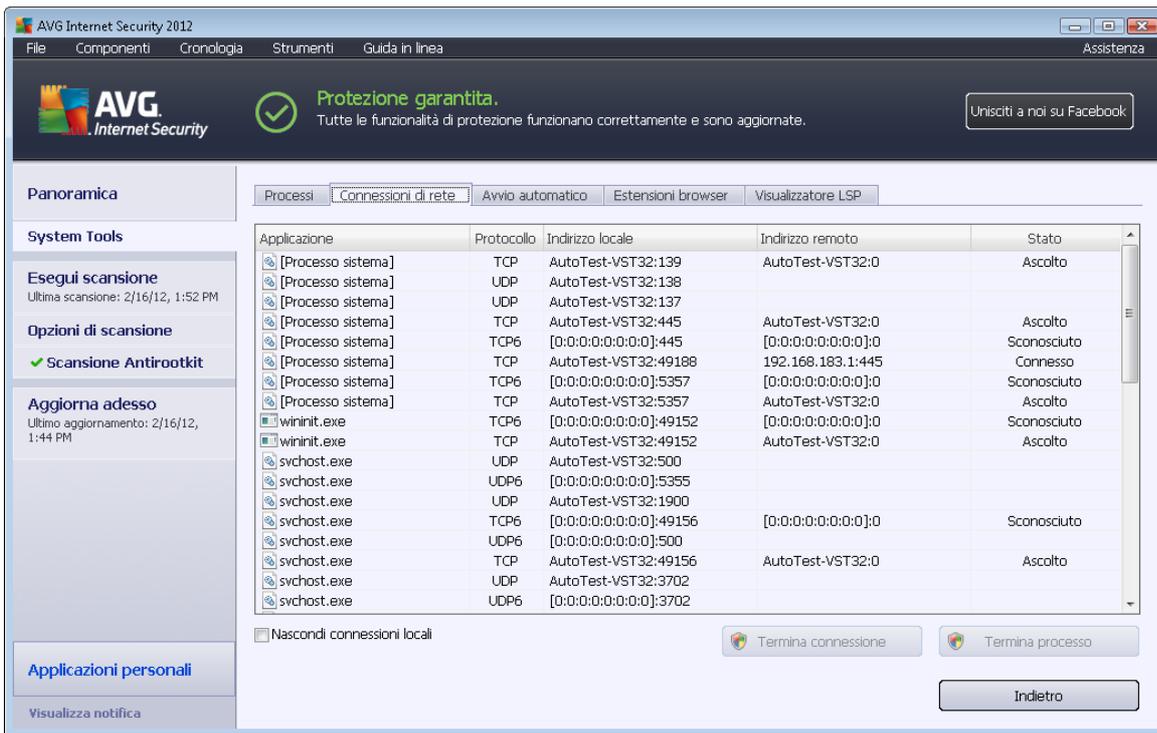
- ***Livello gravità***: identificazione grafica della gravità di un determinato processo valutata su una scala di quattro livelli dal meno grave (■□□□) al più grave (■■■■)
- ***Nome processo***: nome del processo in esecuzione.
- ***Percorso processo***: percorso fisico del processo in esecuzione
- ***Finestra***: se applicabile, indica il nome della finestra dell'applicazione in Windows
- ***PID***: il numero di identificazione del processo è un numero interno di Windows univoco

Pulsanti di controllo

I pulsanti di controllo disponibili nella scheda ***Processi*** sono i seguenti:

- ***Aggiorna***: aggiorna l'elenco dei processi in base allo stato corrente
- ***Termina processo***: è possibile selezionare una o più applicazioni, quindi terminarle facendo clic su questo pulsante. ***Si consiglia di non terminare alcuna applicazione se non si è assolutamente sicuri che rappresenti una reale minaccia.***

- ***Indietro***: consente di tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*)

6.6.2. Connessioni di rete

Nella finestra di dialogo ***Connessioni di rete*** è incluso un elenco di connessioni attualmente attive. L'elenco è suddiviso nelle seguenti colonne:

- ***Applicazione***: nome dell'applicazione correlata alla connessione (*con l'eccezione di Windows 2000 in cui le informazioni non sono disponibili*)
- ***Protocollo***: il tipo di protocollo di trasmissione utilizzato per la connessione:
  - TCP: protocollo utilizzato assieme al protocollo IP (Internet Protocol) per trasmettere le informazioni in Internet
  - UDP: protocollo alternativo al protocollo TCP.
- ***Indirizzo locale***: indirizzo IP del computer locale e numero della porta utilizzata.
- ***Indirizzo remoto***: indirizzo IP del computer remoto e numero della porta a cui viene eseguita la connessione. Se possibile, verrà cercato anche il nome host del computer remoto.
- ***Stato***: indica lo stato corrente più probabile (*Connesso, Il server deve essere chiuso, Ascolto, Chiusura attiva terminata, Chiusura passiva, Chiusura attiva*).

Per visualizzare solo le connessioni esterne, selezionare la casella di controllo ***Nascondi connessioni locali*** nella sezione inferiore della finestra di dialogo sotto l'elenco.

Pulsanti di controllo

I pulsanti di controllo disponibili nella scheda ***Connessioni di rete*** sono i seguenti:

- ***Termina connessione***: consente di chiudere una o più connessioni selezionate nell'elenco.
- ***Termina processo***: consente di chiudere una o più applicazioni correlate alle connessioni selezionate nell'elenco
- ***Indietro***: consente di tornare alla finestra di dialogo principale di AVG predefinita (panoramica dei componenti).

Talvolta è possibile terminare solo le applicazioni il cui stato corrente è Connesso. Si consiglia di non terminare alcuna connessione se non si è assolutamente sicuri che rappresenti una reale minaccia.

6.6.3. Avvio automatico

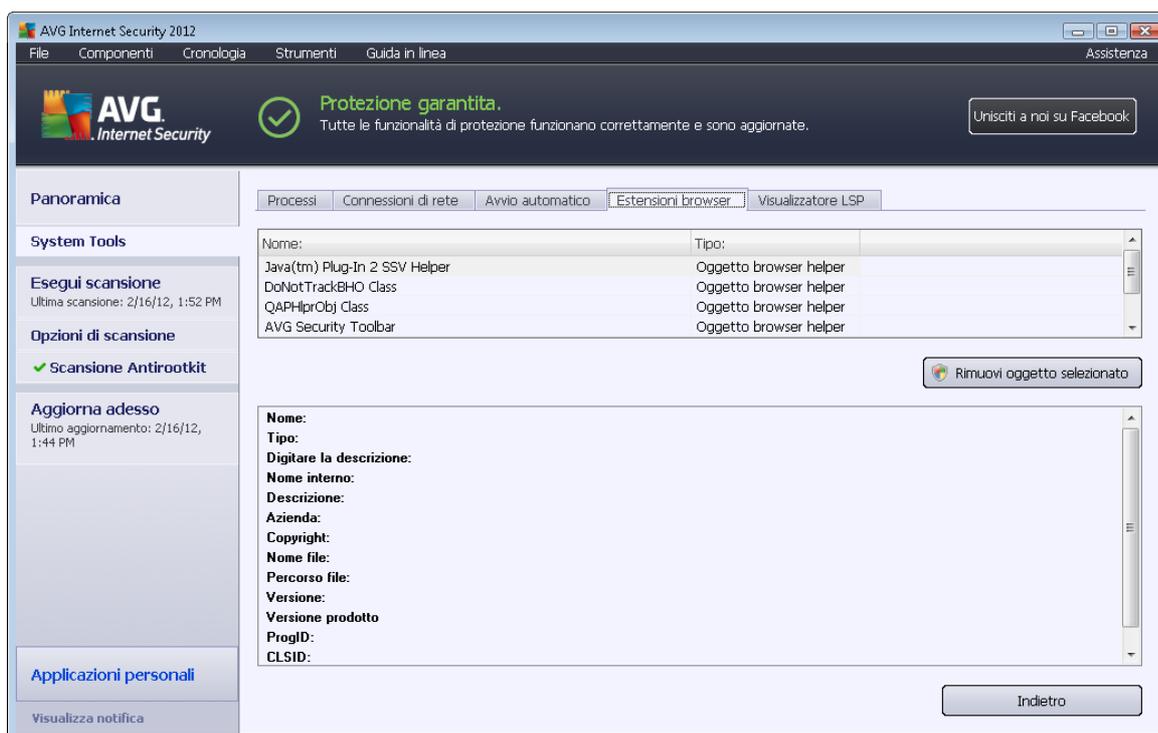
Nella finestra di dialogo ***Avvio automatico*** è visualizzato un elenco di tutte le applicazioni eseguite durante l'avvio del sistema Windows. Molto spesso diverse applicazioni malware si aggiungono automaticamente alle voci del registro di avvio.

Pulsanti di controllo

I pulsanti di controllo disponibili nella scheda ***Avvio automatico*** sono i seguenti:

- ***Rimuovi voci selezionate***: fare clic su questo pulsante per eliminare una o più voci selezionate.
- ***Indietro***: consente di tornare alla finestra di dialogo principale di AVG predefinita *(panoramica dei componenti).*

Si consiglia di non eliminare nessuna applicazione dall'elenco se non si è assolutamente sicuri che rappresenti una reale minaccia.

6.6.4. Estensioni browser

Nella finestra di dialogo ***Estensioni browser*** è presente l'elenco dei plug-in (*applicazioni*) installati nel browser Web. L'elenco può includere normali plug-in delle applicazioni, ma anche potenziali programmi malware. Fare clic su un oggetto dell'elenco per ottenere informazioni dettagliate sul plug-in selezionato, che verranno visualizzate nella sezione inferiore della finestra di dialogo.

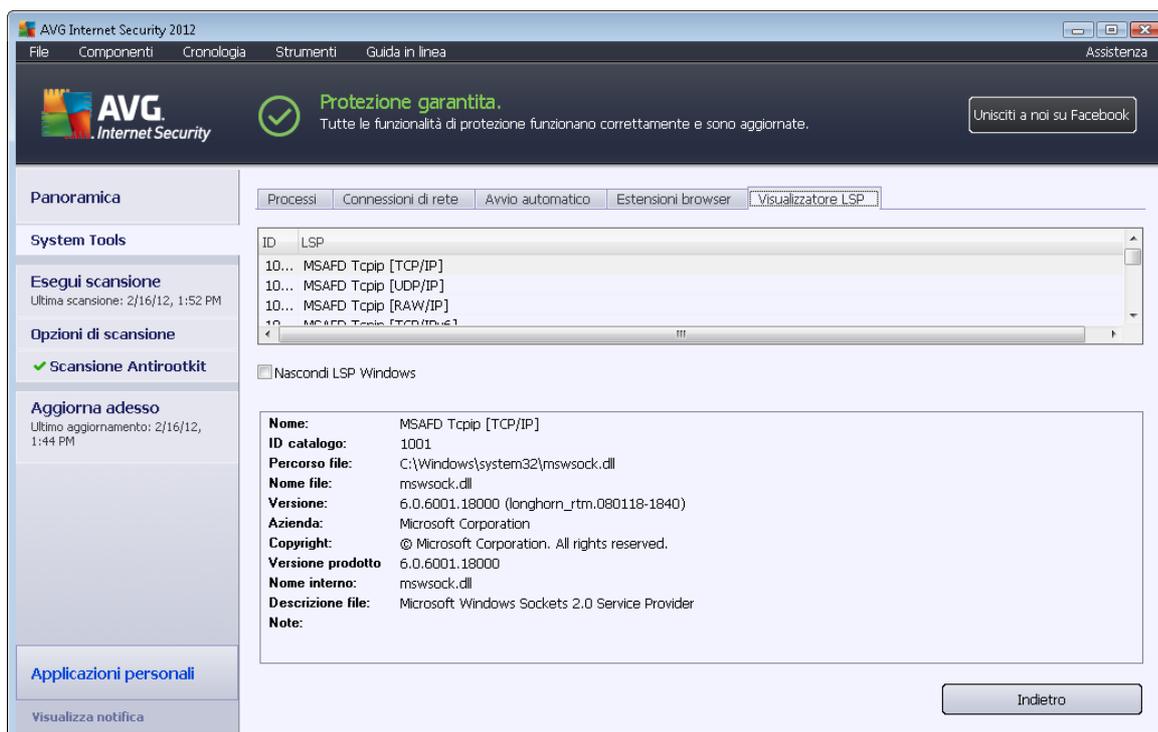
Pulsanti di controllo

I pulsanti di controllo disponibili nella scheda ***Estensioni browser*** sono i seguenti:

- ***Rimuovi oggetto selezionato***: rimuove il plug-in evidenziato nell'elenco. ***Se non si è***

assolutamente sicuri che un plug-in rappresenti una reale minaccia, si consiglia di non eliminarlo dall'elenco.

- ***Indietro***: consente di tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti).*

6.6.5. Visualizzatore LSP

Nella finestra di dialogo ***Visualizzatore LSP*** viene visualizzato un elenco di LSP (Layered Service Provider).

Un ***LSP*** è un driver di sistema collegato ai servizi di rete del sistema operativo Windows. È in grado di accedere a tutti i dati in entrata e in uscita dal computer e di modificare tali dati. Alcuni LSP sono necessari per consentire a Windows di connettere il computer dell'utente ad altri computer e a Internet. Tuttavia, anche alcune applicazioni malware possono installarsi come LSP e in tal modo avere accesso a tutti i dati trasmessi dal computer. Pertanto, questa analisi potrà aiutare l'utente a verificare tutte le possibili minacce LSP.

In determinate circostanze è anche possibile correggere LSP danneggiati (*ad esempio quando il file è stato rimosso ma le voci del Registro di sistema sono rimaste intatte*). Quando viene rilevato un LSP riparabile, viene visualizzato un nuovo pulsante per la correzione del problema.

Pulsanti di controllo

I pulsanti di controllo disponibili nella scheda ***Visualizzatore LSP*** sono i seguenti:

- ***Nascondi LSP Windows***: per includere LSP Windows nell'elenco, deselezionare questa voce.
- ***Indietro***: consente di tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*).

6.7. PC Analyzer

Il componente ***PC Analyzer*** esamina il computer per rilevare problemi di sistema e fornisce una panoramica dettagliata di ciò che potrebbe ridurre le prestazioni globali del computer. Nell'interfaccia utente del componente è possibile visualizzare un grafico diviso in quattro righe relative alle seguenti categorie: errori di registro, file inutili, frammentazione e collegamenti interrotti:

- ***Errori di registro*** fornisce il numero di errori nel Registro di Windows. Poiché la correzione del registro richiede particolare esperienza, non è consigliabile correggere il registro personalmente.
- ***File inutili*** fornisce il numero di file che sono molto probabilmente superflui. In genere si tratta di file temporanei di vario tipo e dei file presenti nel Cestino.
- ***Frammentazione*** consente di calcolare la percentuale di disco rigido frammentata, ovvero utilizzata per molto tempo per cui al momento i file si trovano sparsi in diverse parti del disco fisico. È possibile utilizzare strumenti per la deframmentazione per correggere questa situazione.
- ***Collegamenti interrotti*** indica all'utente collegamenti non più funzionanti, che conducono a posizioni inesistenti e così via.

Per avviare l'analisi del sistema, selezionare il pulsante ***Analizza ora***. Sarà quindi possibile visualizzare l'avanzamento dell'analisi e i relativi risultati direttamente nel grafico:

La panoramica dei risultati fornisce il numero di problemi del sistema rilevati (***Errori***) divisi in base alle categorie controllate. I risultati dell'analisi verranno inoltre visualizzati graficamente nella colonna ***Gravità***.

Pulsanti di controllo

- ***Analizza ora*** (*visualizzato prima dell'avvio dell'analisi*): selezionare questo pulsante per avviare immediatamente l'analisi del computer
- ***Correggi ora*** (*visualizzato al completamento dell'analisi*): selezionare il pulsante per visualizzare il sito Web di AVG (http://www.avg.com/) alla pagina contenente informazioni dettagliate e aggiornate correlate al componente ***PC Analyzer***
- ***Annulla***: selezionare il pulsante per arrestare l'analisi in corso o per tornare alla finestra di dialogo principale di AVG predefinita (*panoramica dei componenti*) al completamento dell'analisi

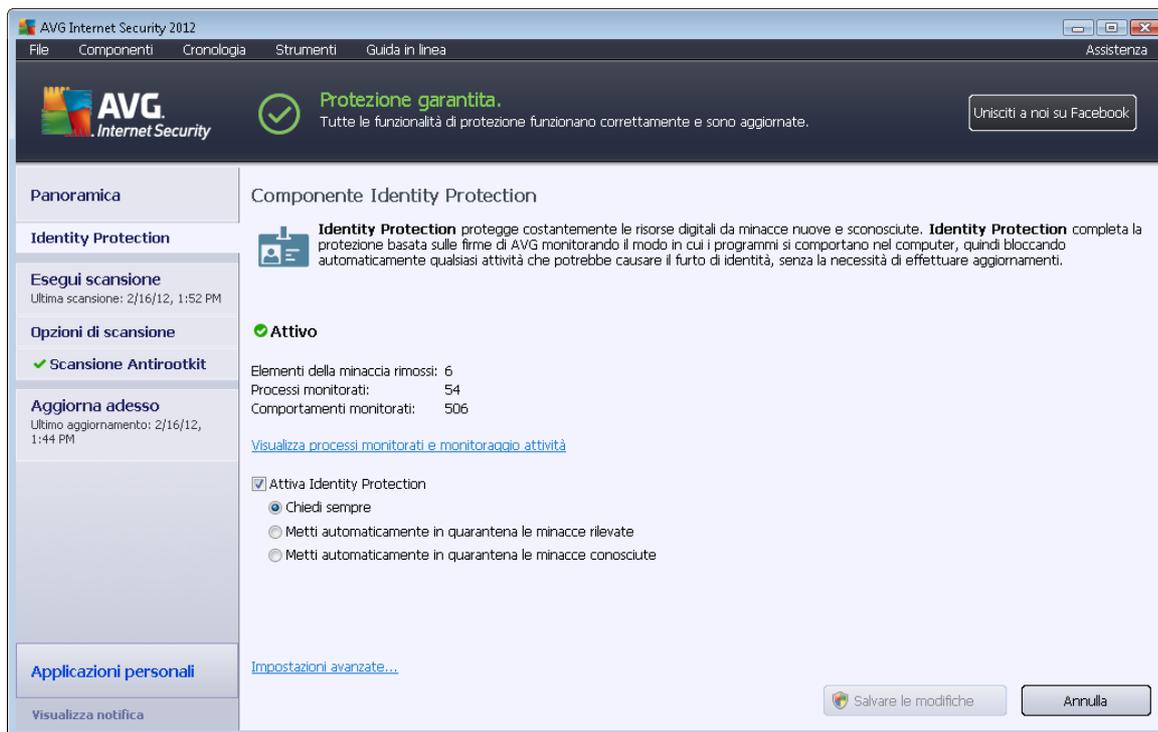
6.8. Identity Protection

Identity Protection è un componente anti-malware che protegge da tutti i tipi di malware (*spyware, bot, furto di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus. ***Identity Protection*** è destinato alla prevenzione di attacchi da parte di malintenzionati volti a sottrarre password, dati dei conti bancari, numeri delle carte di credito

e altri importanti dati digitali tramite qualsiasi tipo di software dannoso (*malware*) in grado di colpire il PC. L'applicazione assicura che tutti i programmi in esecuzione nel PC o nella rete condivisa funzionino correttamente. ***Identity Protection*** rileva e blocca i comportamenti sospetti in modo continuo e protegge il computer da tutti i nuovi malware.

Identity Protection fornisce al computer la protezione in tempo reale da minacce nuove e sconosciute. Monitora tutti i processi *(compresi quelli nascosti)* e oltre 285 diversi schemi di comportamento ed è in grado di determinare se nel sistema si stanno verificando operazioni dannose. Per tale motivo, può rilevare minacce non ancora descritte nel database dei virus. Quando un codice sconosciuto entra nel computer viene immediatamente controllato, per verificarne l'eventuale comportamento dannoso, e tracciato. Se si determina che il file è dannoso, ***Identity Protection rimuove il codice spostandolo in*** Quarantena virus e annulla le modifiche apportate al sistema *(iniezioni di codice, modifiche del registro, apertura di porte e così via)*. Non è necessario avviare una scansione per essere protetti. La tecnologia è proattiva, richiede raramente l'aggiornamento ed è sempre attiva.

Identity Protection costituisce una protezione complementare all'Anti-Virus. È consigliabile installare entrambi i componenti per disporre della protezione completa per il PC.

6.8.1. Interfaccia di Identity Protection

La finestra di dialogo ***Identity Protection*** fornisce una breve descrizione delle funzionalità di base del componente, informazioni sul relativo stato *(Attivo)* e alcuni dati statistici:

- ***Elementi della minaccia rimossi***: numero di applicazioni rilevate come malware e rimosse
- ***Processi monitorati***: numero di applicazioni in esecuzione monitorate da IDP

- ***Comportamenti monitorati***: numero di azioni specifiche in esecuzione all'interno delle applicazioni monitorate

Di seguito è disponibile il collegamento Visualizza processi monitorati e monitoraggio attività che consente di accedere all'interfaccia utente del componente System Tools che include una panoramica dettagliata di tutti i processi monitorati.

Impostazioni di base di Identity Protection

Nella parte inferiore della finestra di dialogo è possibile modificare alcune funzionalità di base del componente:

- ***Attiva Identity Protection*** (*attivata per impostazione predefinita*): selezionare questa opzione per attivare il componente IDP e accedere a opzioni di modifica aggiuntive.

  In alcuni casi, ***Identity Protection*** potrebbe segnalare che un file legittimo è sospetto o pericoloso. Poiché ***Identity Protection*** rileva le minacce in base al comportamento, ciò solitamente accade quando un programma tenta di monitorare la pressione dei tasti o di installare altri programmi oppure quando un nuovo driver viene installato nel computer. Pertanto, selezionare una delle seguenti opzioni specificando il comportamento del componente ***Identity Protection*** in caso di rilevamento di attività sospette:

  - ***Chiedi sempre***: se un'applicazione viene rilevata come malware verrà richiesto se dovrà essere bloccata (*questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo*)

  - ***Metti automaticamente in quarantena le minacce rilevate***: tutte le applicazioni rilevate come malware verranno bloccate automaticamente

  - ***Metti automaticamente in quarantena le minacce conosciute***: solo le applicazioni rilevate come malware con assoluta certezza verranno bloccate

- ***Impostazioni avanzate...***: fare clic sul collegamento per accedere alla relativa finestra di dialogo nelle Impostazioni avanzate di **AVG Internet Security 2012**. In questa finestra di dialogo è possibile modificare la configurazione del componente nei dettagli. Tuttavia, tenere presente che la configurazione predefinita di tutti i componenti è impostata in modo che **AVG Internet Security 2012** offra prestazioni ottimali e il massimo livello di protezione. Si consiglia di mantenere la configurazione predefinita a meno che non siano presenti motivi validi per modificarla.

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di ***Identity Protection*** sono i seguenti:

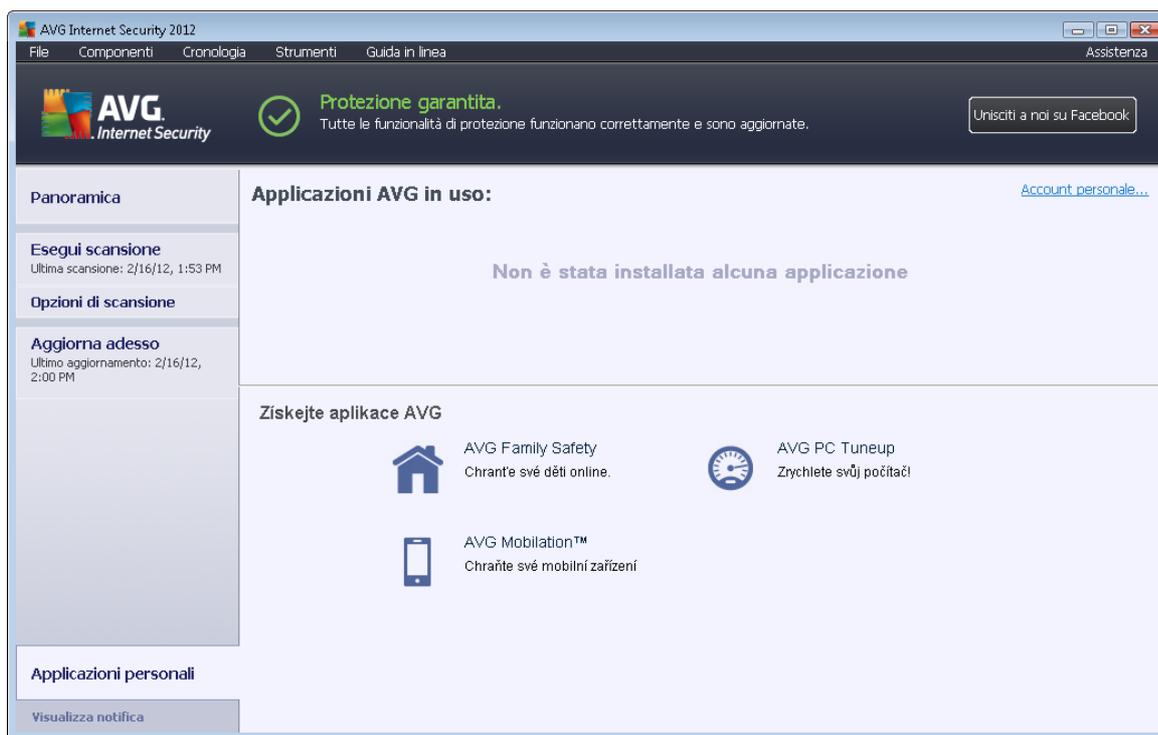
- ***Salva modifiche***: selezionare questo pulsante per salvare e applicare le eventuali modifiche eseguite in questa finestra di dialogo

- ***Annulla***: selezionare questo pulsante per tornare alla finestra di dialogo principale di AVG ***predefinita*** (*panoramica dei componenti*)

6.9. Amministrazione remota

Il componente ***Amministrazione remota*** viene visualizzato nell'interfaccia utente di **AVG Internet Security 2012** se è stata installata la versione Business Edition del prodotto *(per informazioni sulla licenza utilizzata per l'installazione, vedere la scheda Versione della finestra di dialogo Informazioni accessibile tramite la voce del menu di sistema Assistenza)*. Per la descrizione dettagliata di opzioni e funzionalità del componente all'interno del sistema AVG Amministrazione remota, consultare la documentazione specifica dedicata esclusivamente a questo argomento. Questa documentazione è disponibile per il download sul sito Web di AVG (http://www.avg.com/), nella sezione ***Centro di assistenza / Download / Documentazione***.

7. Applicazioni personali

La finestra di dialogo ***Applicazioni personali*** *(accessibile direttamente tramite il pulsante Applicazioni personali dalla finestra di dialogo principale di AVG)* fornisce una panoramica delle applicazioni autonome AVG, incluse quelle già installate nel computer e quelle che è possibile installare facoltativamente:

La finestra di dialogo è suddivisa in due sezioni:

- ***Applicazioni AVG in uso***: fornisce una panoramica delle applicazioni autonome AVG che sono già installate nel computer.
- ***Ottieni le applicazioni AVG***: offre una panoramica delle applicazioni autonome AVG che potrebbero interessare all'utente. Queste applicazioni sono pronte per essere installate. L'offerta varia in modo dinamico in base alla licenza, alla località e ad altri criteri. Per informazioni dettagliate su queste applicazioni, consultare il sito Web di AVG (http://www.avg.com/).

Di seguito viene fornita una panoramica di tutte le applicazioni disponibili e una breve spiegazione delle loro funzionalità:

7.1. AVG Family Safety

AVG Family Safety aiuta a proteggere i bambini da siti Web, ricerche in linea e contenuti multimediali inappropriati e fornisce rapporti relativi alle attività che essi svolgono in linea. ***AVG Family Safety monitora la pressione dei tasti sulla tastiera per controllare le attività dei bambini nelle chat room e sui social network.*** Se rileva parole, frasi o espressioni tipicamente

utilizzati per adescare i bambini in linea, invia una notifica immediata tramite SMS o e-mail. L'applicazione consente di impostare il livello di protezione che meglio si adatta a ciascun bambino e controllarne l'attività separatamente tramite dati di accesso univoci.

Per informazioni dettagliate, visitare la pagina Web AVG dedicata, in cui è inoltre possibile effettuare subito il download del componente. A tale scopo, è possibile utilizzare il collegamento AVG Family Safety all'interno della finestra di dialogo Applicazioni personali.

7.2. AVG LiveKive

AVG LiveKive è destinato al backup dei dati in linea su server sicuri. ***AVG LiveKive*** esegue il backup automatico di tutti i file, le foto e la musica in una posizione sicura, consentendo di condividerli con familiari e amici e di accedervi da qualsiasi dispositivo abilitato per il Web, inclusi dispositivi Android e iPhone. ***AVG LiveKive*** include le seguenti funzionalità:

- Misure di sicurezza nel caso in cui il computer e/o il disco rigido venissero danneggiati
- Accesso ai dati da qualsiasi dispositivo connesso a Internet
- Organizzazione semplificata
- Condivisione con le persone autorizzate

Per informazioni dettagliate, visitare la pagina Web AVG dedicata, in cui è inoltre possibile effettuare subito il download del componente. A tale scopo, è possibile utilizzare il collegamento AVG LiveKive all'interno della finestra di dialogo Applicazioni personali.

7.3. AVG Mobilation

AVG Mobilation protegge i telefoni cellulari da virus e malware, oltre a fornire la capacità di rilevare lo smartphone in modalità remota in caso di necessità. Le funzionalità di ***AVG Mobilation*** includono:

- *File Scanner* abilita la scansione di protezione dei file in diverse posizioni di memorizzazione.
- *Task Killer* consente di arrestare un'applicazione in caso il dispositivo rallenti o si blocchi.
- *App Locker* consente di bloccare e proteggere tramite password una o più applicazioni per evitare utilizzi impropri.
- *Tuneup* raccoglie diversi parametri di sistema *(livello della batteria, spazio di archiviazione utilizzato, dimensioni e percorso delle applicazioni installate e così via)* in un'unica visualizzazione centralizzata per consentire il controllo delle prestazioni del sistema.
- *App Backup* consente di eseguire il backup delle applicazioni sulla scheda SD e di ripristinarle in seguito.
- *Spam e truffe* consente di contrassegnare messaggi SMS come spam e di segnalare siti Web come truffe.

- *Eliminazione dei dati personali* in remoto in caso di furto del telefono.

- *Safe Web Surfing* offre un controllo in tempo reale delle pagine Web visitate.

Per informazioni dettagliate, visitare la pagina Web AVG dedicata, in cui è inoltre possibile effettuare subito il download del componente. Per farlo, è possibile utilizzare il collegamento AVG Mobilation all'interno della finestra di dialogo Applicazioni personali.

7.4. AVG PC Tuneup

L'applicazione ***AVG PC Tuneup*** è uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che consente di migliorare la velocità e le prestazioni generali del computer. ***AVG PC Tuneup*** include le seguenti funzionalità:

- Disk Cleaner: rimuove i file indesiderati che rallentano il computer.
- Disk Defrag: deframmenta i dischi rigidi e ottimizza il posizionamento dei file del sistema.
- Registry Cleaner: corregge gli errori del registro per aumentare la stabilità del PC.
- Registry Defrag: compatta il registro eliminando spazi che causando il consumo di memoria.
- Disk Doctor: identifica settori danneggiati, cluster persi ed errori delle directory e li corregge.
- Internet Optimizer: personalizza le impostazioni generiche per una connessione Internet specifica.
- Track Eraser: rimuove la cronologia dell'uso del computer e di Internet.
- Disk Wiper: pulisce lo spazio libero sui dischi per evitare il recupero di dati sensibili eliminati.
- File Shredder: elimina i file selezionati senza possibilità di recupero su un disco o un'unità USB.
- File Recovery: recupera i file eliminati accidentalmente da dischi, unità USB o fotocamere.
- Duplicate File Finder: ricerca e rimuove file duplicati che consumano spazio su disco.
- Services Manager: disattiva i servizi non necessari che rallentano il computer.
- Startup Manager: consente di gestire i programmi che vengono avviati automaticamente all'avvio di Windows.
- Uninstall Manager: disinstalla completamente i programmi software non più necessari.

- Tweak Manager: consente di regolare centinaia di impostazioni Windows nascoste.
- Task Manager: elenca tutti i processi e i servizi in esecuzione e i file bloccati.
- Disk Explorer: mostra quali file occupano più spazio nel computer.
- System Information: fornisce informazioni dettagliate sull'hardware e il software installati.

Per informazioni dettagliate, visitare la pagina Web AVG dedicata, in cui è inoltre possibile effettuare subito il download del componente. A tale scopo, è possibile utilizzare il collegamento AVG PC Tuneup all'interno della finestra di dialogo Applicazioni personali.

8. AVG Security Toolbar

AVG Security Toolbar è uno strumento che funziona insieme al componente LinkScanner per assicurare la protezione massima durante la navigazione in Internet. All'interno di **AVG Internet Security 2012**, l'installazione di ***AVG Security Toolbar*** è opzionale; durante il processo di installazione viene richiesto se installare o meno il componente. ***AVG Security Toolbar*** è disponibile direttamente nel browser Internet. Al momento, i browser Internet supportati sono Internet Explorer (*versione 6.0 e successive*) e/o Mozilla Firefox (*versione 3.0 e successive*). Non sono supportati altri browser *(se si utilizza un browser Internet alternativo, ad esempio Avant Browser, potrebbero verificarsi comportamenti inattesi)*.

AVG Security Toolbar si compone dei seguenti elementi:

- ***Logo AVG*** con il menu a discesa:
    - ***Usa AVG Secure Search***: consente di effettuare ricerche direttamente da ***AVG Security Toolbar*** utilizzando il motore ***AVG Secure Search***. Tutti i risultati di ricerca vengono controllati di continuo dal servizio Search-Shield per garantire la protezione assoluta in linea.
    - ***Livello di minacce corrente***: consente di aprire la pagina Web di Virus Lab contenente la visualizzazione grafica del livello di minacce corrente sul Web.
    - ***AVG Threat Labs***: apre il sito Web specifico ***AVG Threat Lab*** (*all'indirizzo http://www.avgthreatlabs.com*), dove è possibile ottenere informazioni relative alla sicurezza di vari siti Web e all'attuale livello di rischio in linea.
    - ***Guida di AVG Security Toolbar***: apre la Guida in linea che tratta tutte le funzionalità di ***AVG Security Toolbar***.
    - ***Invia commenti sul prodotto***: apre una pagina Web che contiene un modulo utilizzabile per inviare commenti circa ***AVG Security Toolbar***.
    - ***Informazioni su...***: apre una nuova finestra contenente informazioni sulla versione installata di ***AVG Security Toolbar***.
- ***Campo di ricerca***: consente di effettuare ricerche in Internet utilizzando ***AVG Security Toolbar*** per essere certi che tutti i risultati visualizzati siano sicuri al 100%. Immettere una parola chiave o una frase nel campo di ricerca, quindi fare clic sul pulsante ***Cerca*** *(o premere Invio)*. Tutti i risultati di ricerca vengono controllati di continuo dal servizio Search-Shield *(incluso nel componente LinkScanner)*.

- ***Sicurezza sito***: questo pulsante consente di aprire una nuova finestra di dialogo, che fornisce informazioni sull'attuale livello di rischio (*Attualmente sicuro*) della pagina che si sta visitando. Questa breve panoramica può essere espansa e visualizzata con informazioni complete su tutte le attività di protezione relative alla pagina nella finestra del browser (*Visualizza rapporto completo*):

- ***Elimina***: tramite l'icona del cestino è possibile visualizzare un menu a discesa che consente di scegliere se eliminare le informazioni su navigazione, download e moduli in linea oppure l'intera cronologia ricerche.

- ***Meteo***: il pulsante apre una nuova finestra di dialogo che fornisce informazioni sul meteo nella località di residenza e previsioni per i due giorni successivi. Queste informazioni vengono aggiornate regolarmente ogni 3-6 ore. Nella finestra di dialogo è possibile cambiare la località desiderata manualmente e specificare se visualizzare le informazioni relative alla temperatura in gradi Celsius o Fahrenheit.

- ***Facebook***: questo pulsante consente di effettuare la connessione al social network Facebook direttamente da ***AVG Security Toolbar***

- Pulsanti di scelta rapida per l'accesso rapido alle seguenti applicazioni: ***Calcolatrice***, ***Blocco note***, ***Esplora risorse***.

9. AVG Do Not Track

AVG Do Not Track consente di individuare i siti Web che raccolgono informazioni sulle attività in linea dell'utente. Un'icona nel browser consente di visualizzare i siti Web e gli inserzionisti che raccolgono informazioni sull'attività dell'utente, che può scegliere di consentirli o impedirli.

- ***AVG Do Not Track*** fornisce informazioni aggiuntive sull'informativa sulla privacy di ciascun servizio, oltre a un collegamento che consente di revocare l'adesione al servizio (se disponibile).
- ***AVG Do Not Track*** utilizza inoltre il protocollo W3C DNT per segnalare automaticamente ai siti che l'utente desidera impedire il tracciamento. Questa notifica è abilitata per impostazione predefinita, ma può essere modificata in qualsiasi momento.
- ***AVG Do Not Track*** viene fornito in base a questi termini e condizioni.
- ***AVG Do Not Track è abilitato per impostazione predefinita, ma può essere disabilitato in qualsiasi momento.*** Per le istruzioni dettagliate, vedere l'articolo nella sezione delle domande frequenti Disattivazione della funzionalità AVG Do Not Track.
- Per ulteriori informazioni su ***AVG Do Not Track***, visitare il sito Web di AVG.

La funzionalità ***AVG Do Not Track*** è attualmente supportata nei browser Mozilla Firefox, Chrome e Internet Explorer. *In Internet Explorer l'icona di AVG Do Not Track si trova sul lato destro della barra dei comandi. In caso di problemi di visualizzazione dell'icona di AVG Do Not Track con le impostazioni predefinite del browser, assicurarsi che la barra dei comandi sia stata attivata. Se non è comunque possibile visualizzare l'icona, trascinare la barra dei comandi a sinistra per visualizzare tutte le icone e i pulsanti disponibili sulla barra degli strumenti.*

9.1. Interfaccia di AVG Do Not Track

Mentre l'utente è in linea, ***AVG Do Not Track*** lo avvisa non appena viene rilevata una qualsiasi attività di raccolta delle informazioni. Verrà visualizzata la finestra di dialogo seguente:

Tutti i servizi di raccolta delle informazioni rilevati vengono elencati per nome nel riepilogo ***Tracker in questa pagina***. Esistono tre tipi di attività di raccolta delle informazioni riconosciuti da ***AVG Do Not Track***:

- ***Web Analytics*** *(consentiti per impostazione predefinita):* servizi utilizzati per l'ottimizzazione delle prestazioni e dell'esperienza nel relativo sito Web. Questa categoria include servizi come Google Analytics, Omniture o Yahoo Analytics. Si consiglia di non bloccare i servizi di Web Analytics, poiché il sito Web potrebbe non funzionare correttamente.

- ***Social button*** *(consentiti per impostazione predefinita):* elementi progettati per il miglioramento dell'esperienza nei social network. I social button sono i pulsanti che alcuni social network inseriscono in altri siti con l'intento di raccogliere informazioni sull'attività in linea degli utenti che eseguono l'accesso. Alcuni esempi di social button sono i plugin e i pulsanti di Facebook, Twitter e Google.

- ***Ad Network*** *(alcuni sono bloccati per impostazione predefinita):* servizi che raccolgono o condividono informazioni sull'attività in linea dell'utente in più siti, sia direttamente che indirettamente, al fine di offrire contenuti pubblicitari personalizzati, diversamente dalle inserzioni basate sul contenuto. I dettagli di tale processo vengono definiti nell'informativa sulla privacy disponibile nel sito di ciascuna Ad Network. Alcuni servizi Ad Network sono bloccati per impostazione predefinita.

Nota: *in base ai servizi eseguiti in background nel sito Web, alcune di queste sezioni potrebbero non essere visualizzate nella finestra di AVG Do Not Track.*

Nella finestra di dialogo sono inoltre disponibili due collegamenti:

- ***Che cos'è il tracciamento?*** - Facendo clic su questo collegamento nella parte superiore della finestra di dialogo si viene reindirizzati a una pagina Web dedicata che fornisce informazioni dettagliate sui principi del rilevamento e una descrizione dei diversi tipi di rilevamento.

- ***Impostazioni*** - Facendo clic su questo collegamento nella parte superiore della finestra di dialogo si viene reindirizzati a una pagina Web dedicata in cui è possibile configurare vari parametri di ***AVG Do Not Track*** *. Per informazioni dettagliate, vedere il capitolo* *Impostazioni di AVG Do Not Track*.

9.2. Informazioni sui processi di rilevamento

L'elenco dei servizi di raccolta delle informazioni individuati fornisce solo il nome di ogni servizio. Per decidere in modo efficace se bloccare o consentire un determinato servizio, potrebbero essere necessarie ulteriori informazioni. Spostare il mouse sulla voce dell'elenco desiderata. Viene visualizzato un riquadro con informazioni dettagliate sul servizio. In questo modo, è possibile sapere se il servizio raccoglie i dati personali, o altre informazioni disponibili, e se i dati raccolti vengono condivisi con terze parti e archiviati per essere utilizzati in seguito.

Nella parte inferiore del riquadro informativo è disponibile il collegamento ***Informativa sulla privacy***, che reindirizza al sito Web dedicato all'informativa sulla privacy del corrispondente servizio rilevato.

9.3. Blocco dei processi di rilevamento

Gli elenchi Social button, Ad Network e Web Analytics consentono di controllare quali servizi devono essere bloccati. È possibile procedere in due modi:

- ***Blocca tutto*** : fare clic su questo pulsante nella parte inferiore della finestra di dialogo per impedire tutte le attività di raccolta delle informazioni. *Nota: questa azione potrebbe compromettere il funzionamento della pagina Web dove il servizio è in esecuzione.*

- Se non si desidera bloccare contemporaneamente tutti i servizi rilevati, è possibile specificare per ogni servizio se deve essere consentito o bloccato. È possibile consentire l'esecuzione di alcuni dei sistemi rilevati *(ad esempio, Web Analytics)*, che utilizzano i dati raccolti per l'ottimizzazione del sito Web, favorendo il miglioramento dell'ambiente Internet per tutti gli utenti. Tuttavia, è possibile bloccare contemporaneamente le attività di raccolta delle informazioni da parte di tutti i processi classificati come Ad Network. È sufficiente fare clic sull'icona accanto al servizio per bloccare la raccolta delle informazioni *(il nome del processo verrà visualizzato barrato)* o consentirla nuovamente.

9.4. Impostazioni di AVG Do Not Track

Nella finestra di ***AVG Do Not Track*** è presente una sola opzione di configurazione, ovvero la casella di controllo ***Avvisa quando vengono rilevati tracker attivi***, disponibile nella parte inferiore della finestra. Per impostazione predefinita, questo elemento è disattivato. Selezionare questa casella di controllo per ricevere una notifica ogni volta che si accede a una pagina Web contenente un nuovo servizio di raccolta delle informazioni che non è ancora stato bloccato. Quando è selezionata, se nella pagina che si sta visitando viene individuato un nuovo servizio di raccolta delle informazioni, ***AVG Do Not Track*** visualizza la finestra di dialogo di notifica. In caso contrario, la presenza del

nuovo servizio rilevato verrà segnalata solo dal ***cambiamento di colore*** (da verde a giallo) dell'*icona di AVG Do Not Track*, disponibile sulla barra dei comandi del browser.

Nella parte inferiore della finestra di ***AVG Do Not Track*** è comunque disponibile il collegamento ***Impostazioni***. Facendo clic su questo collegamento si accede a una pagina Web in cui è possibile specificare in modo dettagliato le ***opzioni di AVG Do Not Track***:

- ***Posizione della notifica*** *(per impostazione predefinita, nell'angolo superiore destro)* : aprire il menu a discesa per specificare la posizione desiderata per la finestra di ***AVG Do Not Track*** sullo schermo.

- ***Visualizza notifica per*** *(per impostazione predefinita, il valore è 10)* : in questo campo è possibile specificare l'intervallo di tempo *(in secondi)* per cui la notifica di ***AVG Do Not Track*** deve essere visualizzata. È possibile specificare un valore compreso tra 0 e 60 secondi. *Se il valore specificato è 0, la notifica non viene visualizzata*.

- ***Avvisa quando vengono rilevati tracker attivi*** *(deselezionata per impostazione predefinita)*: selezionare questa casella di controllo per ricevere una notifica ogni volta che si accede a una pagina Web contenente un nuovo servizio di rilevamento che non è ancora stato bloccato. Quando è selezionata, se nella pagina che si sta visitando viene individuato un nuovo servizio di raccolta delle informazioni, ***AVG Do Not Track*** visualizza la finestra di

dialogo di notifica. In caso contrario, la presenza del nuovo servizio rilevato verrà segnalata solo dal ***cambiamento di colore*** (da verde a giallo) dell'*icona di AVG Do Not Track, disponibile sulla barra dei comandi del browser.*

- ***Notifica siti Web per cui disabilitare il tracciamento*** *(selezionata per impostazione predefinita)* : lasciare selezionata questa opzione se si desidera che ***AVG Do Not Track*** informi il provider di un servizio di raccolta delle informazioni che si desidera impedire il tracciamento.

- ***Blocca i seguenti elementi*** *(tutti i servizi di raccolta delle informazioni elencati sono consentiti per impostazione predefinita)*: in questa sezione è possibile visualizzare un riquadro con l'elenco dei servizi di raccolta dati noti classificabili come Ad Network. Per impostazione predefinita, ***AVG Do Not Track*** blocca automaticamente alcune Ad Network ed è possibile scegliere se bloccare anche le restanti o se mantenerle abilitate. A tale scopo, fare clic sul pulsante ***Blocca tutto*** sotto l'elenco.

Nella pagina ***Opzioni di AVG Do Not Track*** sono disponibili i seguenti pulsanti di opzione:

- ***Blocca tutto***: selezionare per bloccare contemporaneamente tutti i servizi elencati nella casella precedente e classificati come Ad Network.

- ***Consenti tutto***: selezionare per sbloccare contemporaneamente tutti i servizi bloccati elencati nella casella precedente e classificati come Ad Network.

- ***Impostazioni predefinite***: selezionare per eliminare tutte le impostazioni personalizzate e ripristinare la configurazione predefinita.

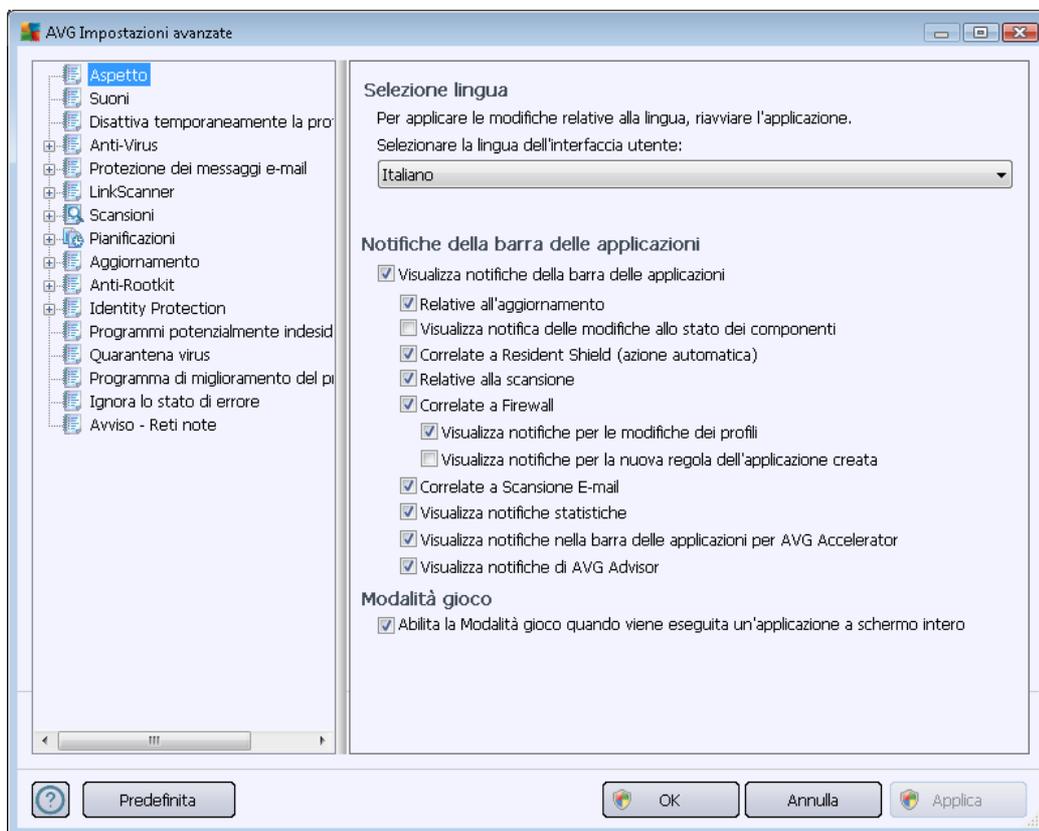
- ***Salva***: fare clic per applicare e salvare la configurazione specificata.

- ***Annulla***: fare clic per annullare tutte le impostazioni precedentemente specificate.

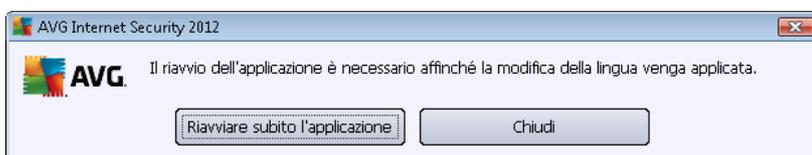
10. Impostazioni AVG avanzate

Le opzioni di configurazione avanzata di **AVG Internet Security 2012** sono disponibili in una nuova finestra denominata ***Impostazioni AVG avanzate***. La finestra è suddivisa in due sezioni: la parte sinistra fornisce una struttura di esplorazione per accedere alle opzioni di configurazione del programma. Selezionare il componente di cui si desidera modificare la configurazione (*o una parte specifica*) per aprire la finestra di dialogo di modifica nella sezione destra della finestra.

10.1. Aspetto

La prima voce della struttura di esplorazione, ***Aspetto***, fa riferimento alle impostazioni generali dell' interfaccia utente di **AVG Internet Security 2012** e fornisce alcune opzioni di base relative al comportamento dell'applicazione:

Selezione lingua

Nella sezione ***Selezione lingua*** è possibile scegliere la lingua desiderata dal menu a discesa. La lingua selezionata verrà quindi utilizzata per l'intera interfaccia utente di **AVG Internet Security 2012**. Nel menu a discesa sono presenti solo le lingue selezionate in precedenza per essere installate durante il processo di installazione (*vedere il capitolo relativo alle opzioni personalizzate*) e l'inglese (*sempre installato automaticamente per impostazione predefinita*). Per completare l'impostazione di **AVG Internet Security 2012** su un'altra lingua è necessario riavviare l'applicazione. Procedere come segue:

- Nel menu a discesa, selezionare la lingua desiderata per l'applicazione
- Confermare la selezione facendo clic sul pulsante ***Applica*** *(angolo inferiore destro della finestra di dialogo)*
- Fare clic sul pulsante ***OK*** per confermare
- Viene visualizzata una nuova finestra di dialogo che comunica che per modificare la lingua dell'applicazione è necessario riavviare **AVG Internet Security 2012**
- Fare clic su pulsante ***Riavviare subito l'applicazione*** per confermare il riavvio del programma e attendere alcuni istanti l'applicazione della modifica della lingua:

Notifiche della barra delle applicazioni

In questa sezione è possibile eliminare la visualizzazione delle notifiche della barra delle applicazioni sullo stato dell'applicazione **AVG Internet Security 2012**. Per impostazione predefinita, le notifiche della barra delle applicazioni vengono visualizzate. Si consiglia di mantenere questa impostazione. Le notifiche di sistema comunicano, ad esempio, l'avvio del processo di scansione o aggiornamento o una modifica dello stato di un componente di **AVG Internet Security 2012**. Questi avvisi devono essere tenuti nella dovuta considerazione.

Tuttavia, se per qualche ragione non si desidera visualizzare tali notifiche o si desidera visualizzarne solo alcune *(correlate a un componente AVG Internet Security 2012 specifico)*, è possibile definire e specificare le proprie preferenze selezionando/deselezionando le opzioni seguenti:

- ***Visualizza notifiche della barra delle applicazioni*** *(attivata per impostazione predefinita)* : per impostazione predefinita, tutte le notifiche vengono visualizzate. Deselezionare questa voce per disattivare completamente la visualizzazione delle notifiche di sistema. Quando è attivata, è possibile selezionare inoltre le notifiche specifiche da visualizzare:
  - ***Visualizza notifiche della barra delle applicazioni relative all'aggiornamento*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative all'avvio, all'avanzamento e alla finalizzazione del processo di aggiornamento di **AVG Internet Security 2012**.
  - ***Visualizza notifica delle modifiche allo stato dei componenti*** *(disattivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative allo stato di attività/inattività del componente o a un suo eventuale problema. Quando viene riportato lo stato di errore di un componente, questa opzione equivale alla funzione informativa dell'icona della barra delle applicazioni per indicare un problema di un componente di **AVG Internet Security 2012**.
  - ***Visualizza notifiche della barra delle applicazioni correlate a Resident Shield***

(azione automatica)*(attivata per impostazione predefinita)*: consente di decidere se visualizzare o meno le informazioni relative ai processi di salvataggio, copia e apertura dei file (*questa configurazione è disponibile solo se l'opzione Correzione automatica di Resident Shield è attiva*).

- ***Visualizza notifiche della barra delle applicazioni relative alla scansione*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative all'avvio automatico, all'avanzamento e ai risultati della scansione pianificata.

- ***Visualizza notifiche della barra delle applicazioni correlate a Firewall*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative ai processi e allo stato del firewall, quali avvisi di attivazione/disattivazione del componente, possibile blocco del traffico e così via. Questa voce fornisce altre due opzioni di selezione specifiche *(per la spiegazione dettagliata di ciascuna di esse consultare il capitolo Firewall di questo documento)*:

  - ***Visualizza notifiche per le modifiche dei profili*** *(attivata per impostazione predefinita)*: informa circa modifiche automatiche ai profili Firewall.

  - ***Visualizza notifiche per la nuova regola dell'applicazione creata*** *(disattivata per impostazione predefinita)*: comunica all'utente la creazione automatica di regole Firewall per nuove applicazioni in base a un elenco di applicazioni sicure.

- ***Visualizza notifiche della barra delle applicazioni correlate a Scansione E-mail*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative alla scansione di tutti i messaggi e-mail in entrata e in uscita.

- ***Visualizza notifiche statistiche*** *(attivata per impostazione predefinita)*: mantenere l'opzione selezionata per consentire la visualizzazione di regolari notifiche delle revisioni statistiche nella barra delle applicazioni.

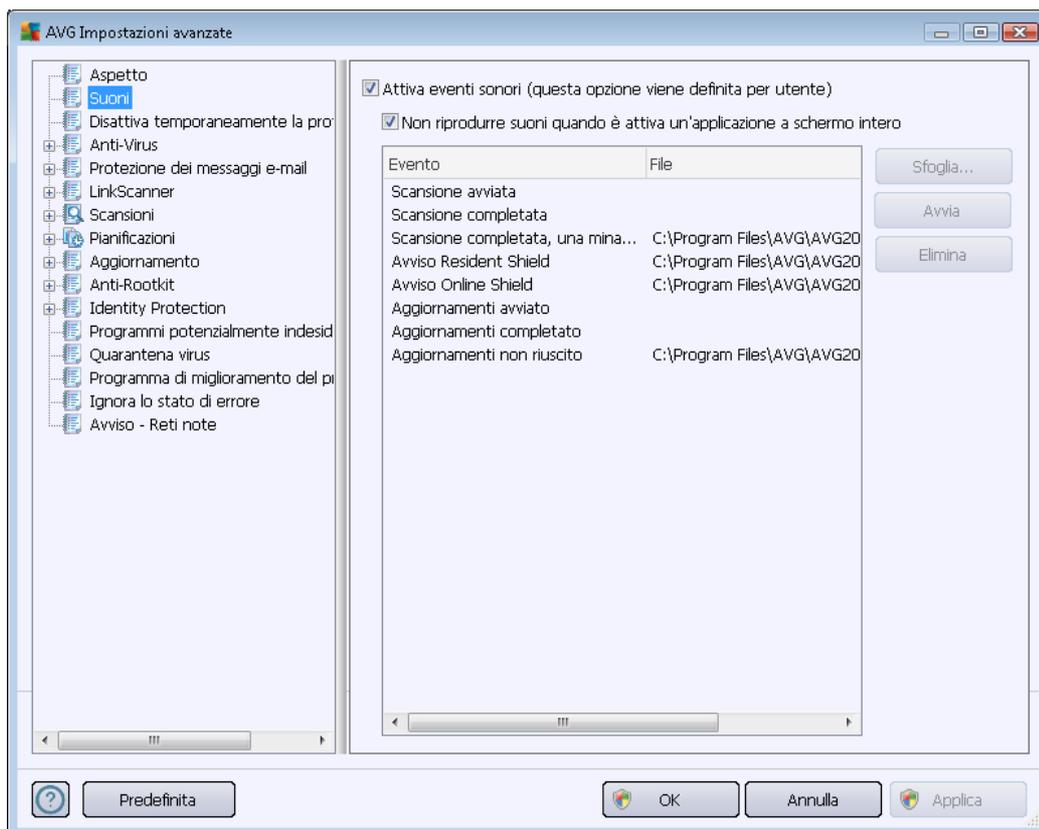
- ***Visualizza notifiche nella barra delle applicazioni per AVG Accelerator*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative alle attività di ***AVG Accelerator***. ***AVG Accelerator*** è un servizio che ottimizza la riproduzione dei video in linea e semplifica il download.

- ***Visualizza notifiche sulle prestazioni di AVG Advice*** *(attivata per impostazione predefinita)*: ***AVG Advice*** controlla le prestazioni dei browser Internet supportati *(Internet Explorer, Chrome, Firefox, Opera e Safari)* e informa l'utente se il browser utilizza una quantità di memoria superiore a quella consigliata. In tali situazioni, le prestazioni del computer potrebbero venire notevolmente rallentate; è consigliabile riavviare il browser Internet per velocizzare i processi. Mantenere attivata la voce ***Visualizza notifiche sulle prestazioni di AVG Advice*** per ricevere le relative informazioni.

Modalità gioco

Questa funzione di AVG è stata progettata per le applicazioni a schermo intero, per le quali eventuali notifiche tramite fumetto di AVG (*visualizzate ad esempio all'avvio di una scansione pianificata*) potrebbero rappresentare una fonte di disturbo (*riducendole a icona o alterandone la grafica*). Per evitare questa situazione, mantenere selezionata la casella di controllo dell'opzione ***Abilita la modalità gioco quando viene eseguita un'applicazione a schermo intero*** (*impostazione predefinita*).

10.2. Suoni

Nella finestra di dialogo ***Suoni*** è possibile specificare se si desidera essere informati circa specifiche azioni di **AVG Internet Security 2012** tramite una notifica sonora:

Le impostazioni sono valide solo per l'account utente corrente, pertanto ogni utente del computer può disporre di impostazioni dei suoni personalizzate. Per consentire le notifiche sonore, mantenere l'opzione ***Attiva eventi sonori*** selezionata (*l'opzione è attivata per impostazione predefinita*) per attivare l'elenco di tutte le azioni correlate. Inoltre, è possibile selezionare l'opzione ***Non riprodurre suoni quando è attiva un'applicazione a schermo intero*** per eliminare le notifiche sonore quando potrebbero essere di disturbo *(vedere anche la sezione relativa alla modalità gioco del capitolo* *Impostazioni avanzate/Aspetto* *in questo documento).*

Pulsanti di controllo

- ***Sfoglia***: dopo aver selezionato l'evento dall'elenco, utilizzare il pulsante ***Sfoglia*** per ricercare nel disco il file audio desiderato da assegnargli *(al momento sono supportati solo file *.wav).*
- ***Avvia***: per ascoltare il suono selezionato, evidenziare l'evento nell'elenco e fare clic sul pulsante ***Avvia***.
- ***Elimina***: utilizzare il pulsante ***Elimina*** per rimuovere il suono assegnato a uno specifico

evento.

10.3. Disattiva temporaneamente la protezione di AVG

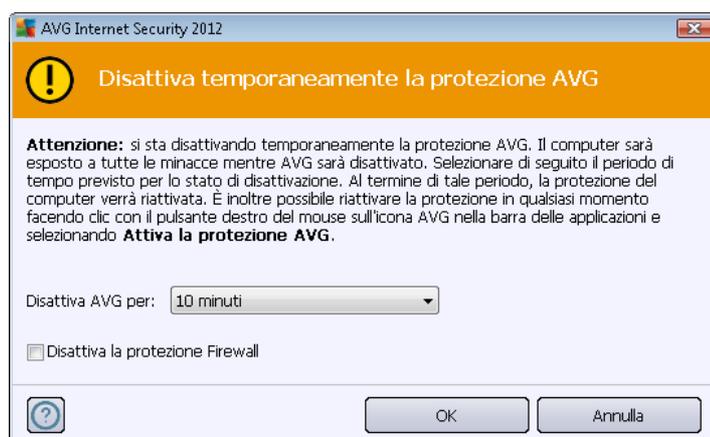
Nella finestra di dialogo ***Disabilitare temporaneamente la protezione di AVG*** è possibile disattivare l'intera protezione fornita da **AVG Internet Security 2012**.

Non utilizzare questa opzione se non è assolutamente necessario.

Nella maggior parte dei casi, ***non è necessario*** disattivare **AVG Internet Security 2012** prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. In caso di problemi durante l'installazione, provare innanzitutto a disattivare la protezione permanente (*Abilita Resident Shield*). Se fosse necessario disattivare temporaneamente **AVG Internet Security 2012**, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.

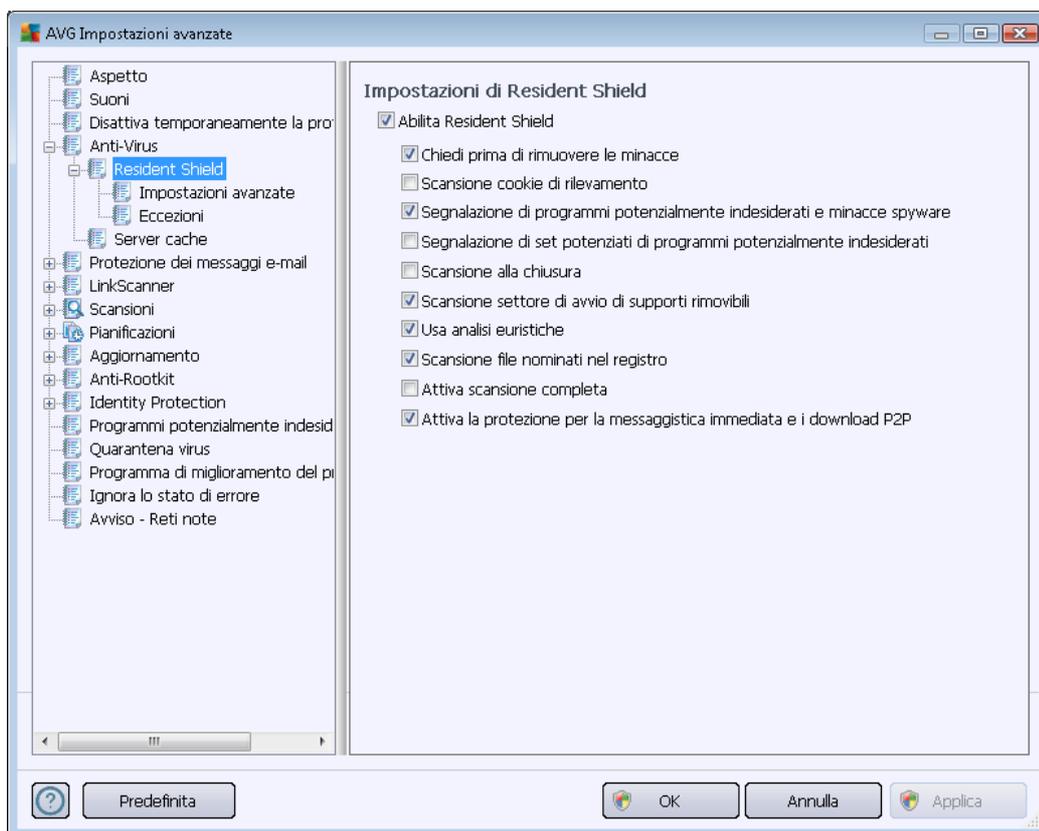
Come disattivare la protezione AVG

- Selezionare la casella di controllo ***Disattiva temporaneamente la protezione di AVG*** e confermare la scelta facendo clic sul pulsante ***Applica***

- Nella finestra di dialogo ***Disattiva temporaneamente la protezione di AVG*** aperta, specificare per quanto tempo si desidera disattivare **AVG Internet Security 2012**. Per impostazione predefinita, la protezione verrà disattivata per 10 minuti, tempo sufficiente per svolgere attività comuni quali l'installazione di nuovo software e così via. Tenere presente che il limite di tempo iniziale che è possibile impostare è pari a 15 minuti e non può essere sostituito da un valore personalizzato per motivi di sicurezza. Una volta trascorso l'intervallo di tempo specificato, tutti i componenti disattivati verranno riattivati automaticamente.

10.4. Anti-Virus

Il componente ***Anti-Virus***protegge il computer in modo continuo da tutti i tipi noti di virus e spyware *(inclusi di cosiddetti malware dormienti e inattivi, ovvero i malware che sono stati scaricati ma non sono ancora stati attivati)*.

10.4.1. Resident Shield

Resident Shield fornisce la protezione attiva di file e cartelle contro virus, spyware e altro malware.

Nella finestra di dialogo ***Impostazioni di Resident Shield*** è possibile attivare o disattivare completamente la protezione permanente selezionando/deselezionando la voce ***Abilita Resident Shield*** (*questa opzione è attivata per impostazione predefinita*). Inoltre, è possibile selezionare quali funzionalità della protezione permanente devono essere attivate:

- ***Chiedi prima di rimuovere le minacce*** (attiva per impostazione predefinita): selezionando questa opzione, Resident Shield non eseguirà alcuna azione automaticamente. Verrà invece visualizzata una finestra di dialogo che descrive la minaccia rilevata, consentendo di scegliere l'azione da eseguire. Se si mantiene deselezionata la casella, **AVG Internet Security 2012** tenterà automaticamente di correggere l'infezione e, nel caso sia impossibile, sposterà l'oggetto in Quarantena virus.

- ***Scansione cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione (*i cookie HTTP sono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti e il contenuto dei carrelli elettronici*).

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un

rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione alla chiusura*** (*disattivata per impostazione predefinita*): la scansione alla chiusura assicura che AVG esegua la scansione di oggetti attivi (ad esempio applicazioni, documenti e così via) quando vengono aperti e anche quando vengono chiusi; questa funzionalità consente di proteggere il computer da alcuni tipi di virus sofisticati.

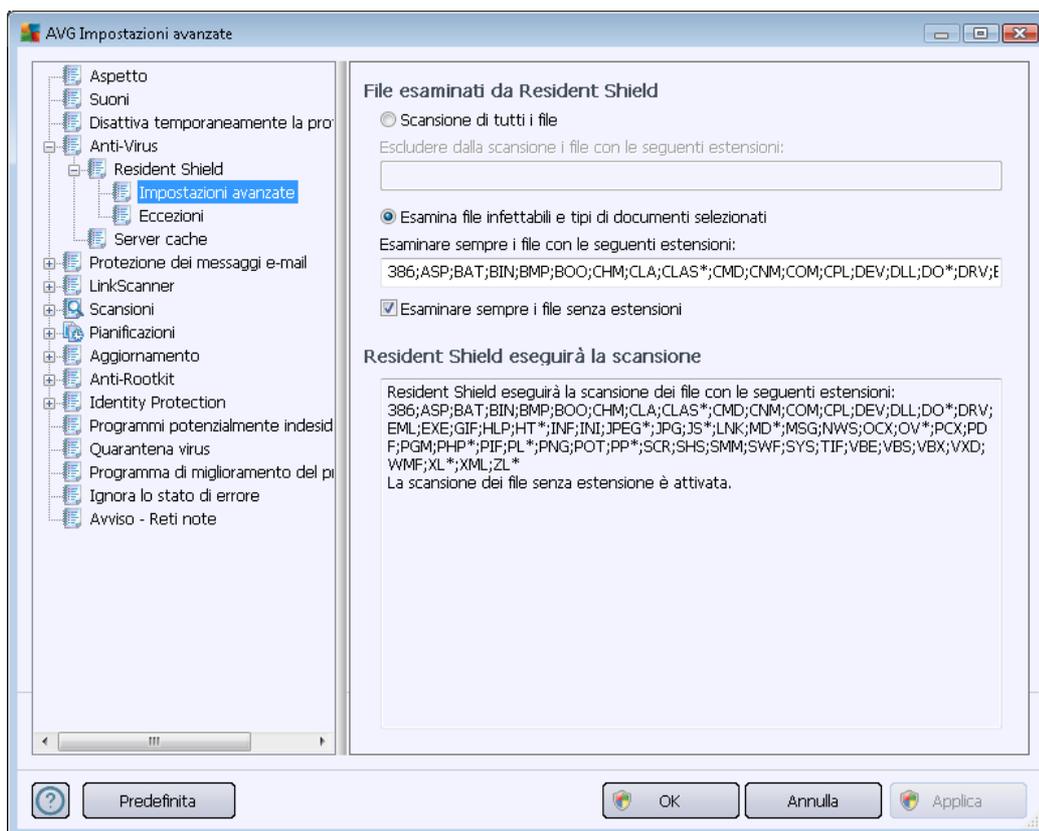
- ***Scansione settore di avvio di supporti rimovibili*** (*attivata per impostazione predefinita*)

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica verrà utilizzata per il rilevamento (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

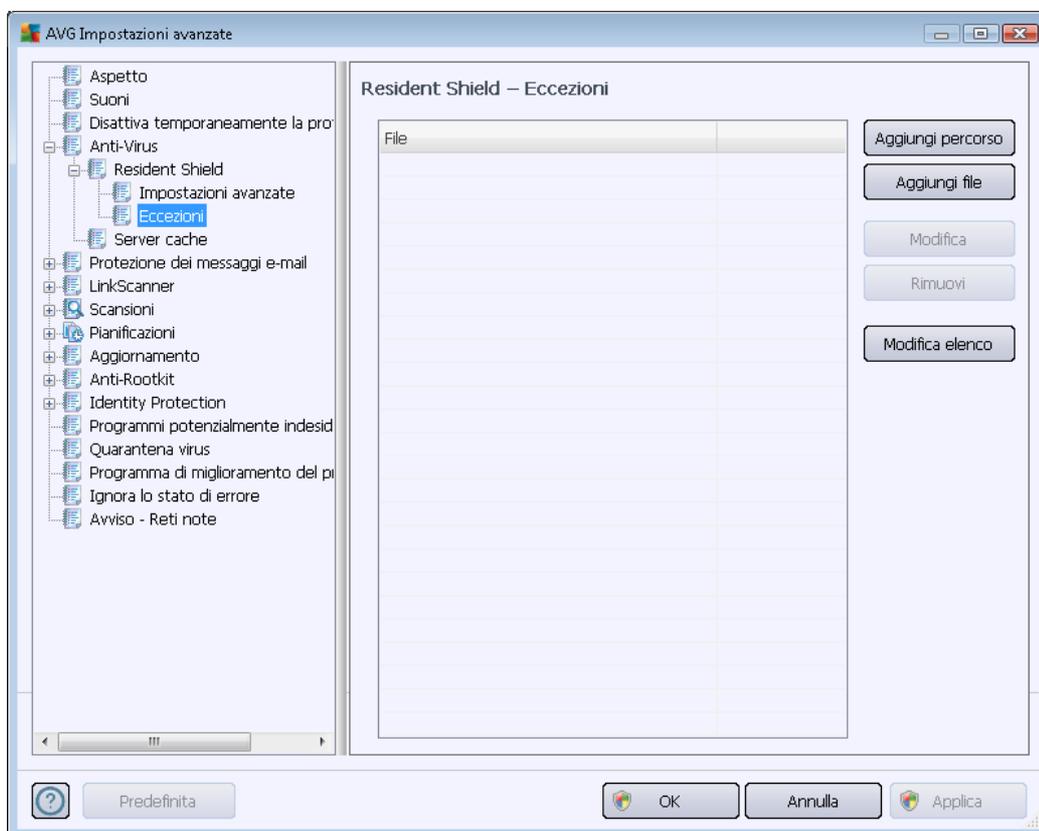
- ***Scansione file nominati nel registro*** (*attivata per impostazione predefinita*): questo parametro specifica che AVG sottoporrà a scansione tutti i file eseguibili aggiunti al registro di avvio per evitare che un'infezione nota venga eseguita al successivo avvio del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*stati di estrema emergenza*) è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno accuratamente tutti gli oggetti potenzialmente minacciosi. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Attiva la protezione per la messaggistica immediata e i download P2P*** (*attivata per impostazione predefinita*): selezionare questa voce per verificare che le comunicazioni di messaggistica immediata (*ad esempio ICQ, MSN Messenger e così via*) e i download P2P siano privi di virus.

Nella finestra di dialogo ***File esaminati da Resident Shield*** è possibile configurare i file che verranno sottoposti a scansione (*in base a estensioni specifiche*):

Selezionare la casella di controllo pertinente per specificare se si desidera utilizzare l'opzione ***Scansione di tutti i file*** oppure l'opzione ***Esamina file infettabili e tipi di documenti selezionati***. Se è stata scelta la seconda opzione, è possibile specificare un elenco di estensioni che definiscono i file da escludere dalla scansione, nonché un elenco di estensioni che definiscono i file da sottoporre a scansione in qualsiasi caso.

Selezionare l'opzione ***Esaminare sempre i file senza estensioni*** (*attiva per impostazione predefinita*) per assicurare che Resident Shield esegua anche la scansione dei file senza estensione e di formato sconosciuto. Si consiglia di mantenere questa funzionalità sempre attivata, in quanto i file senza estensione sono sospetti.

La seguente sezione ***Oggetto dell'esame di Resident Shield*** fornisce un'ulteriore panoramica dettagliata degli elementi che verranno effettivamente sottoposti a scansione da ***Resident Shield***.

La finestra di dialogo ***Resident Shield – Eccezioni*** consente di definire i file e/o le cartelle che devono essere esclusi dalla scansione ***Resident Shield***.

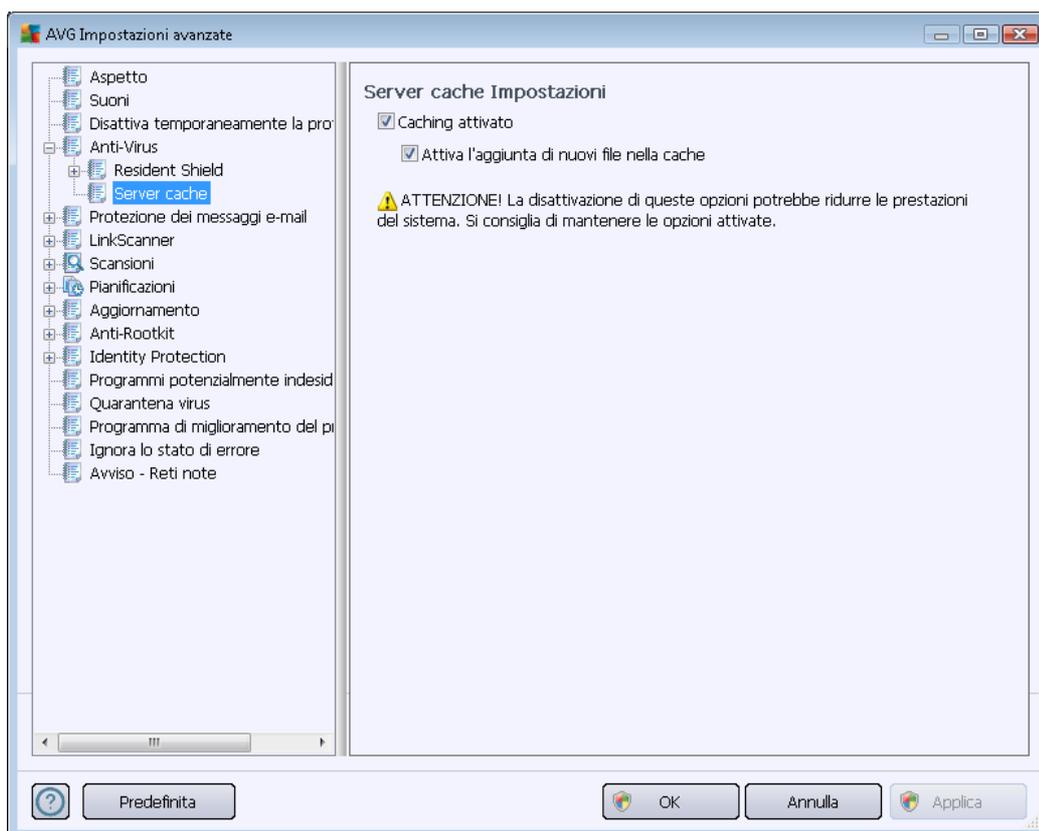
Se non è essenziale, si consiglia di non escludere alcun elemento.

Pulsanti di controllo

La finestra di dialogo fornisce i seguenti pulsanti di controllo:

- ***Aggiungi percorso***: consente di specificare le directory da escludere dalla scansione selezionandole una alla volta dalla struttura di esplorazione del disco locale
- ***Aggiungi file***: consente di specificare i file da escludere dalla scansione selezionandoli uno alla volta dalla struttura di esplorazione del disco locale
- ***Modifica elemento***: consente di modificare il percorso specificato di un file o una cartella selezionati
- ***Rimuovi elemento***: consente di eliminare dall'elenco il percorso dell'elemento selezionato
- ***Modifica elenco***: consente di modificare l'intero elenco delle eccezioni definite in una nuova finestra di dialogo utilizzabile come un editor di testo standard

10.4.2. Server cache

La finestra di dialogo ***Impostazioni del Server cache*** si riferisce al processo server cache destinato a velocizzare tutti i tipi di scansione di **AVG Internet Security 2012**:

Il server cache raccoglie e mantiene le informazioni relative ai file affidabili (*un file viene considerato affidabile se presenta la firma digitale di una fonte affidabile*). Questi file vengono quindi considerati sicuri e non necessitano di ulteriore scansione, pertanto vengono ignorati durante le scansioni.

La finestra di dialogo ***Impostazioni del Server cache*** offre le seguenti opzioni di configurazione:

- ***Caching attivato*** (*attivata per impostazione predefinita*) – deselezionare la casella per disattivare il ***Server cache*** e svuotare la memoria cache. Tenere presente che la scansione potrebbe subire un rallentamento e le prestazioni complessive del computer potrebbero ridursi, poiché per prima cosa ogni singolo file in uso verrà sottoposto alla scansione antivirus e antispyware.

- ***Attiva l'aggiunta di nuovi file nella cache*** (*attivata per impostazione predefinita*) – deselezionare la casella per arrestare l'aggiunta di ulteriori file nella memoria cache. Tutti i file già presenti nella cache verranno mantenuti e utilizzati finché l'inserimento nella cache non verrà disattivato completamente o finché non verrà eseguito il successivo aggiornamento del database dei virus.

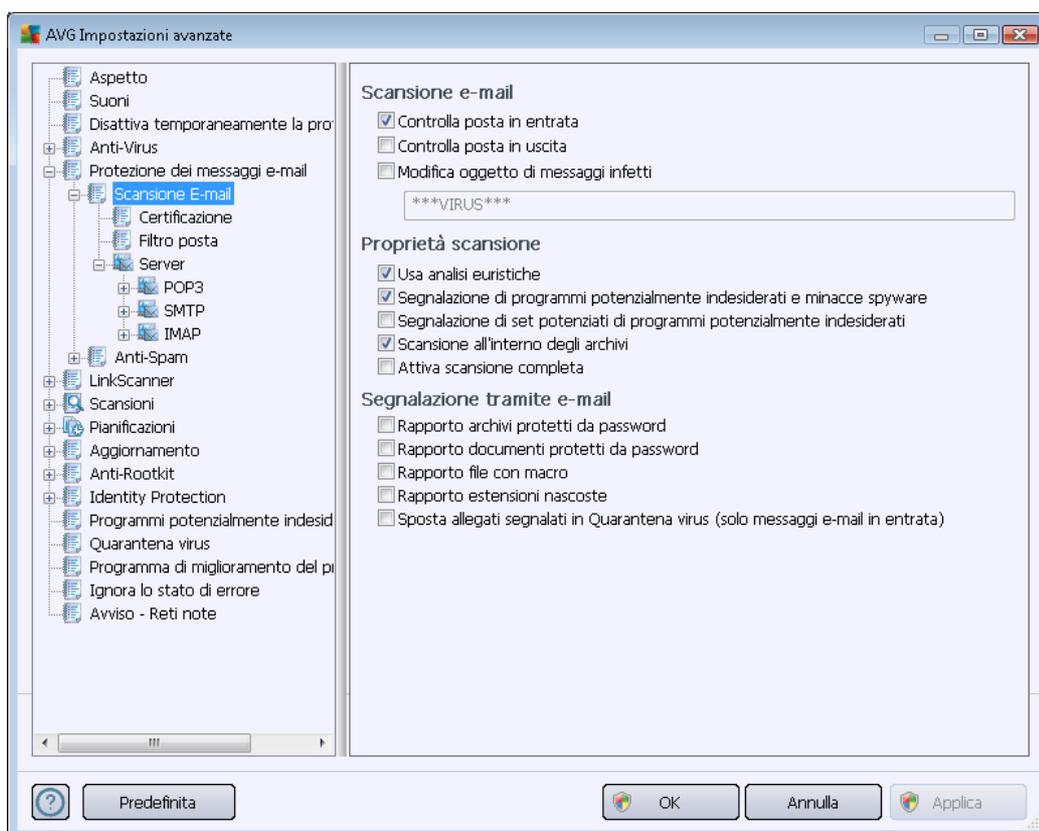
A meno che non sussista un motivo valido per disattivare il server cache, si consiglia di mantenere le impostazioni predefinite e lasciare attivate entrambe le opzioni. In caso

contrario, la velocità e le prestazioni del sistema potrebbero ridursi notevolmente.

10.5. Protezione dei messaggi e-mail

Nella sezione ***Protezione dei messaggi e-mail*** è possibile modificare la configurazione dettagliata di Scansione E-mail e Anti-Spam:

10.5.1. Scansione E-mail

La finestra di dialogo ***Scansione E-mail*** è suddivisa in tre sezioni:

Scansione e-mail

In questa sezione è possibile configurare le seguenti impostazioni di base per i messaggi e-mail in arrivo e/o in uscita:

- ***Controlla posta in entrata*** (*attivata per impostazione predefinita*): selezionare per attivare/ disattivare l'opzione di scansione di tutti i messaggi e-mail consegnati al client e-mail
- ***Controlla posta in uscita*** (*disattivata per impostazione predefinita*): selezionare per attivare/disattivare l'opzione di scansione di tutti i messaggi e-mail inviati dall'account e-mail
- ***Modifica oggetto di messaggi infetti*** (*disattivata per impostazione predefinita*): per essere informati del fatto che il messaggio e-mail esaminato si è rivelato infetto, selezionare questa voce e immettere il testo desiderato nel campo di testo. Il testo verrà aggiunto al campo

"Oggetto" di ogni messaggio rilevato come infetto per facilitarne l'identificazione e il filtro. Il valore predefinito è ***VIRUS***. Si consiglia di mantenere questa impostazione.

Proprietà scansione

In questa sezione è possibile specificare la modalità di scansione dei messaggi e-mail:

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per utilizzare il metodo di rilevamento tramite analisi euristica durante la scansione dei messaggi e-mail. Se questa opzione è attivata, è possibile filtrare gli allegati dei messaggi e-mail non solo per estensione ma anche in base al contenuto effettivo dell'allegato. Il filtro può essere impostato nella finestra di dialogo Filtro posta.

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione all'interno degli archivi*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per eseguire la scansione del contenuto degli archivi allegati ai messaggi e-mail.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato da un virus o un exploit*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

Segnalazione allegati e-mail

In questa sezione, è possibile impostare rapporti aggiuntivi sui file potenzialmente pericolosi o sospetti. Notare che non verrà visualizzato alcun messaggio di avviso, verrà soltanto aggiunto un testo di certificazione alla fine del messaggio e-mail e tutti i rapporti verranno elencati nella finestra di dialogo Rilevamento Scansione E-mail:

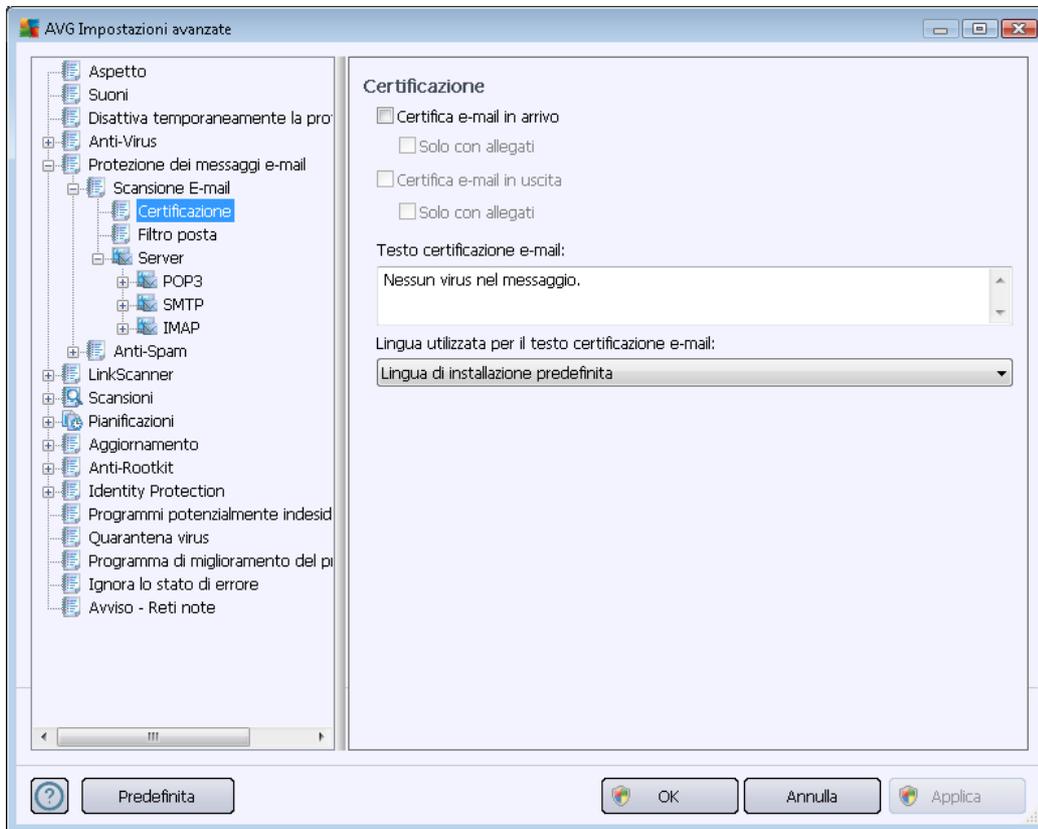
- ***Segnala archivi protetti da password***: gli archivi (*ZIP, RAR e così via*) protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

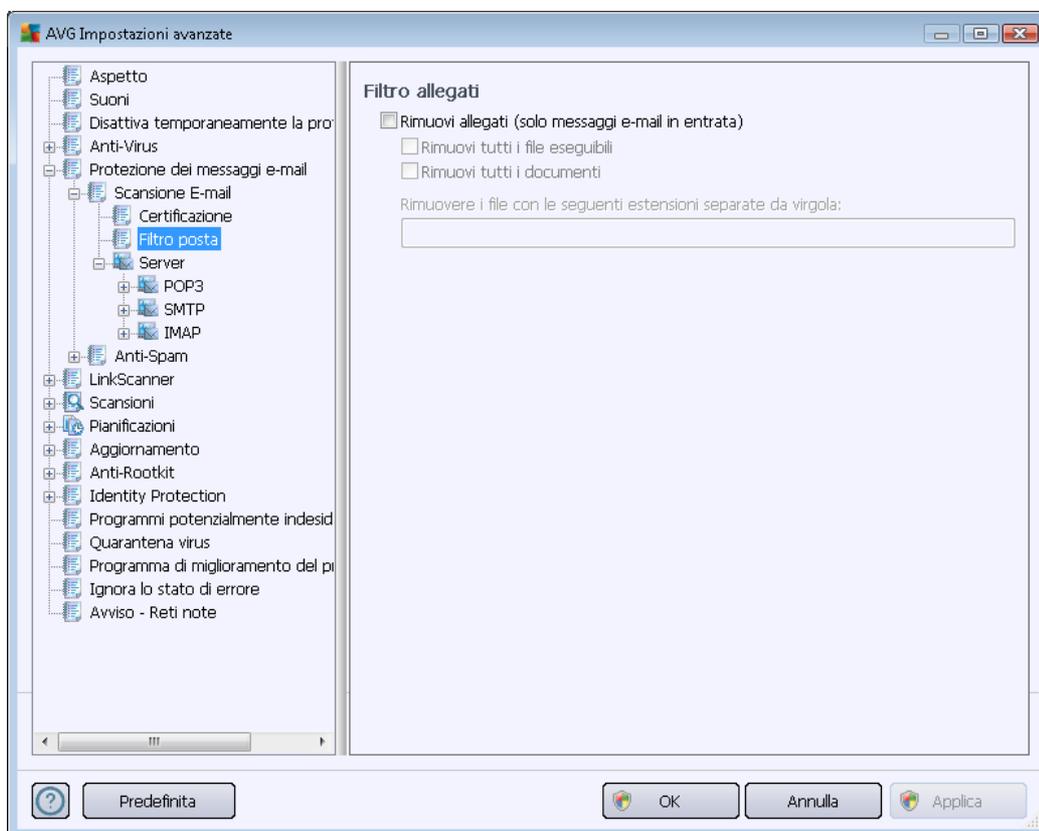
- ***Segnala documenti protetti da password***: i documenti protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

- ***Segnala file contenenti macro***: una macro è una sequenza di passaggi predefinita che consente di semplificare determinate attività (*le macro di MS Word, ad esempio, sono ampiamente conosciute*). Le macro possono contenere istruzioni potenzialmente pericolose. Selezionare la casella di controllo per assicurare che i file contenenti macro vengano segnalati come potenzialmente pericolosi.

- ***Segnala estensioni nascoste***: le estensioni nascoste possono far sembrare un file eseguibile sospetto, ad esempio "nomefile.txt.exe", un innocuo file di testo, ad esempio "nomefile.txt". Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

- ***Sposta allegati segnalati in Quarantena virus***: specifica se si desidera ricevere una notifica via e-mail per gli archivi protetti da password, i documenti protetti da password, i file contenenti macro e/o i file con estensione nascosta rilevati come allegato del messaggio e-mail sottoposto a scansione. Se viene identificato un messaggio simile durante la scansione, è possibile stabilire se l'oggetto infetto rilevato deve essere spostato in Quarantena virus.

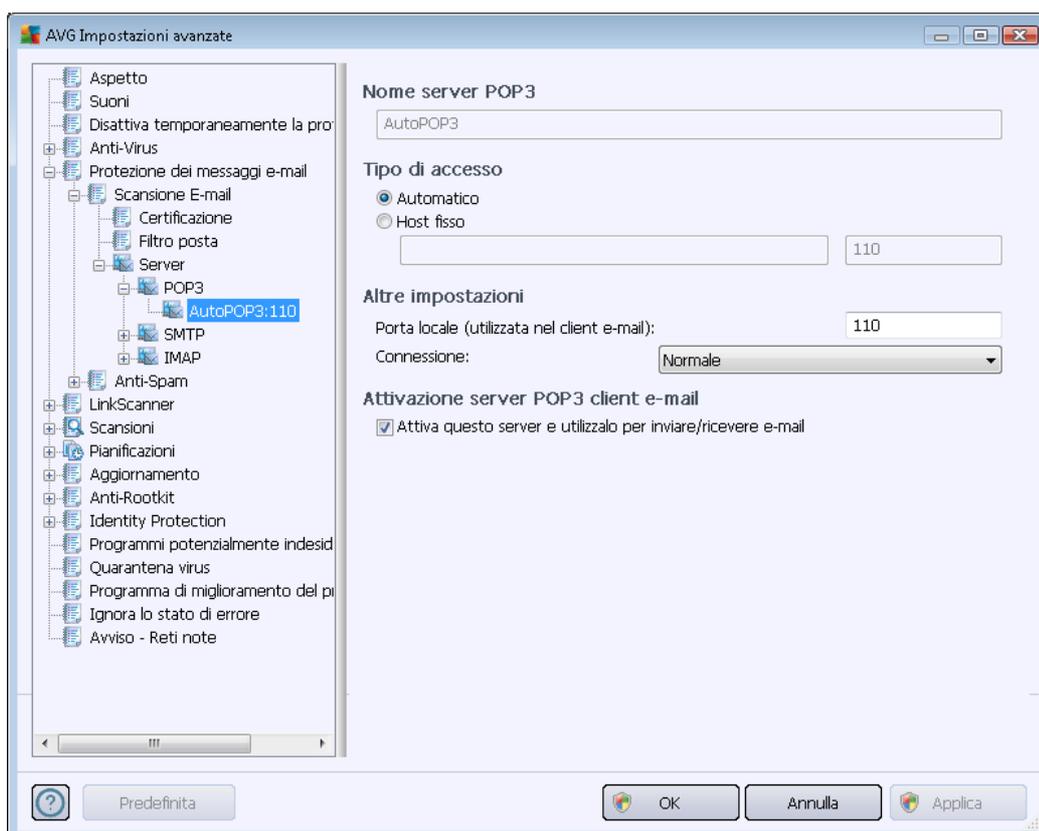
Nella finestra di dialogo ***Certificazione*** è possibile selezionare le caselle di controllo specifiche per specificare se si desidera certificare la posta in arrivo (***Certifica e-mail in arrivo***) e/o la posta in uscita (***Certifica e-mail in uscita***). Per ciascuna di queste opzioni è inoltre possibile specificare il parametro ***Solo con allegati*** per far sì che la certificazione venga aggiunta solo ai messaggi e-mail con allegati:

Per impostazione predefinita, il testo di certificazione è composto da informazioni di base simili a *Nessun virus in questo messaggio.* Tuttavia, è possibile estendere o modificare queste informazioni in base alle esigenze, scrivendo il testo di certificazione desiderato nel campo ***Testo certificazione e-mail***. Nella sezione ***Lingua utilizzata per il testo certificazione e-mail*** è possibile definire inoltre in quale lingua la parte di certificazione generata automaticamente (*Nessun virus in questo messaggio*) verrà visualizzata.

Nota: *tenere presente che solo il testo predefinito verrà visualizzato nella lingua richiesta e il testo personalizzato non verrà tradotto automaticamente.*

La finestra di dialogo ***Filtro allegati*** consente di impostare i parametri per la scansione degli allegati dei messaggi e-mail. Per impostazione predefinita, l'opzione ***Rimuovi allegati*** è disattivata. Se si decide di attivarla, tutti gli allegati dei messaggi e-mail rilevati come infetti o potenzialmente pericolosi verranno rimossi automaticamente. Se si desidera definire tipi specifici di allegati che devono essere rimossi, selezionare l'opzione corrispondente:

- ***Rimuovi tutti i file eseguibili***: tutti i file *.exe verranno eliminati
- ***Rimuovi tutti i documenti***: tutti i file *.doc, *.docx, *.xls e *.xlsx verranno eliminati
- ***Rimuovere i file con le seguenti estensioni separate da virgola***: verranno rimossi tutti i file con le estensioni specificate

Nella sezione ***Server*** è possibile modificare i parametri dei server di Scansione E-mail:

- Server POP3
- Server SMTP
- Server IMAP

Inoltre, è possibile definire un nuovo server per la posta in ingresso o in uscita, utilizzando il pulsante ***Aggiungi nuovo server***.

Questa finestra di dialogo (*che si apre da **Server / POP3***) consente di impostare un nuovo server di Scansione E-mail utilizzando il protocollo POP3 per la posta in entrata:

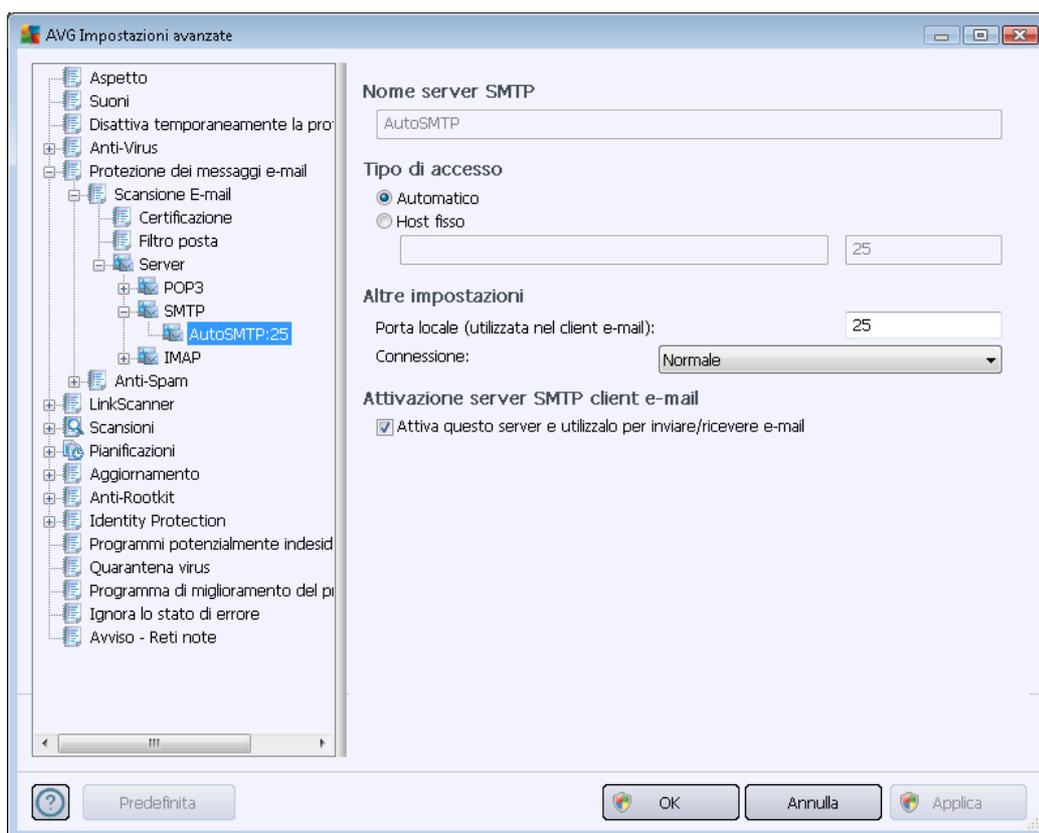
- ***Nome server POP3***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server POP3, fare clic con il pulsante destro del mouse sulla voce POP3 nel menu di esplorazione a sinistra*). Per i server "AutoPOP3" creati automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in entrata:

    - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail.

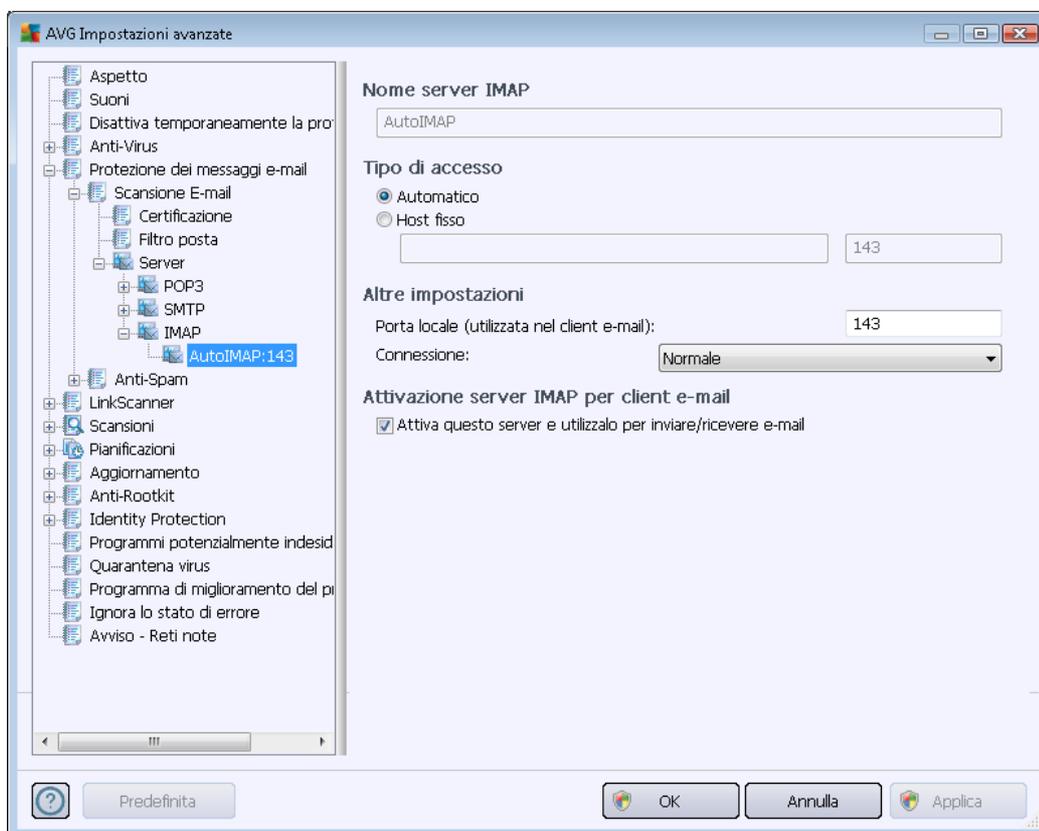
    - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Il nome di accesso non verrà modificato. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio pop.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail utilizza una porta non standard, è possibile specificare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, *ad esempio pop.*

acme.com:8200. La porta standard per la comunicazione POP3 è la numero 110.

- ***Altre impostazioni***: specifica parametri più dettagliati:
  - ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione POP3.
  - ***Connessione***: nel menu a discesa è possibile specificare il tipo di connessione da utilizzare (*regolare/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità inoltre è disponibile solo se supportata dal server e-mail di destinazione.
- ***Attivazione server POP3 client e-mail***: selezionare/deselezionare questa voce per attivare o disattivare il server POP3 specificato

Questa finestra di dialogo (*che si apre tramite **Server / SMTP***) consente di impostare un nuovo server di Scansione E-mail che utilizza il protocollo SMTP per la posta in uscita:

- ***Nome server SMTP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server SMTP, fare clic con il pulsante destro del mouse sulla voce SMTP nel menu di esplorazione a sinistra*). Per i server "AutoSMTP" creati

automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in uscita:
    - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail
    - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, *ad esempio smtp.acme.com:8200*. La porta standard per la comunicazione SMTP è la numero 25.
- ***Altre impostazioni***: specifica parametri più dettagliati:
    - ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione SMTP.
    - ***Connessione***: questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità è disponibile solo se supportata dal server e-mail di destinazione.
- ***Attivazione server SMTP client e-mail***: selezionare/deselezionare questa casella per attivare/disattivare il server SMTP specificato

Questa finestra di dialogo (accessibile tramite ***Server / IMAP***) consente di impostare un nuovo server Scansione E-mail che utilizza il protocollo IMAP per la posta in uscita:

- ***Nome server IMAP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server IMAP, fare clic con il pulsante destro del mouse sulla voce IMAP nel menu di esplorazione a sinistra*). Per i server "AutoIMAP" creati automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server e-mail utilizzato per la posta in uscita:

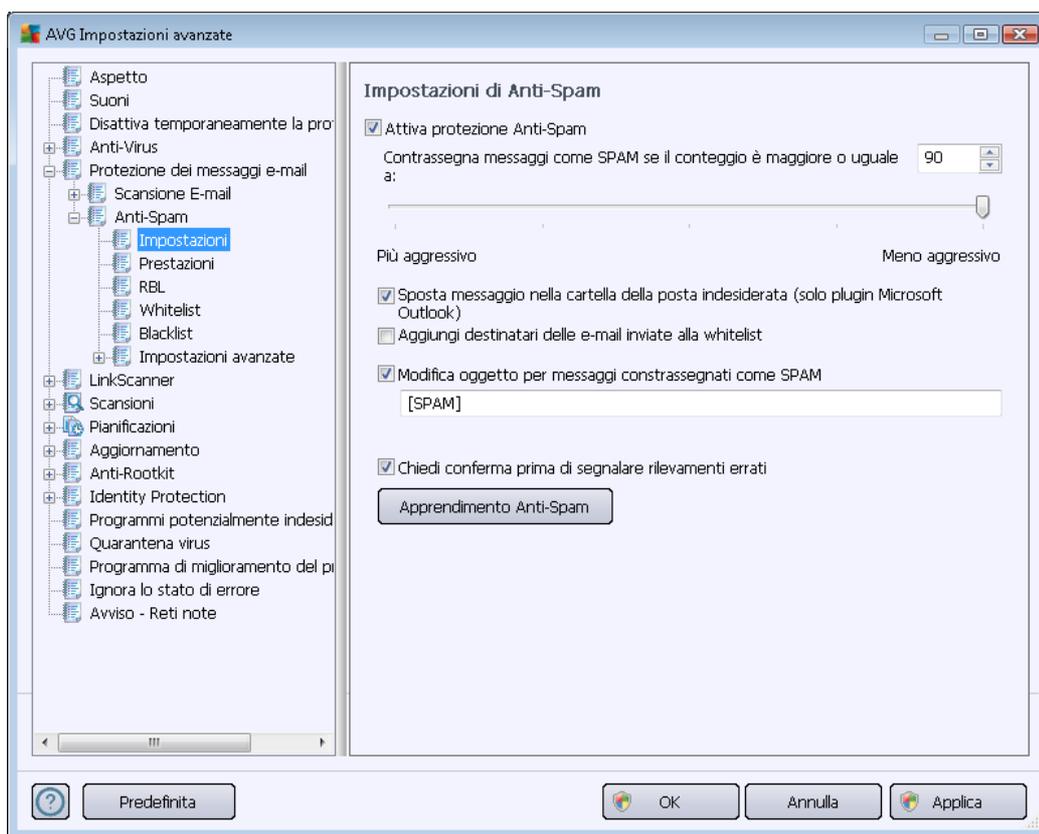
    - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client e-mail

    - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server e-mail. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server e-mail utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, *ad esempio imap.acme.com:8200*. La porta standard per la comunicazione IMAP è la numero 143.

- ***Altre impostazioni***: specifica parametri più dettagliati:

- ○ ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione e-mail. Nell'applicazione e-mail sarà quindi necessario specificare tale porta come porta per la comunicazione IMAP.
- ○ ***Connessione***: questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità è disponibile solo se supportata dal server e-mail di destinazione.

- ***Attivazione server IMAP client e-mail***: selezionare/deselezionare questa casella per attivare/disattivare il server IMAP specificato

10.5.2. Anti-Spam

Nella finestra di dialogo delle ***impostazioni Anti-Spam*** è possibile selezionare/deselezionare la casella di controllo ***Attiva protezione Anti-Spam*** per consentire/impedire la scansione anti-spam delle comunicazioni e-mail. Questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo.

Quindi, è anche possibile selezionare il grado di "aggressività" della configurazione del conteggio. Il filtro ***Anti-Spam*** assegna a ciascun messaggio un conteggio (*ad esempio, il grado di somiglianza del contenuto del messaggio a SPAM*) in base a diverse tecniche di scansione dinamica. È possibile regolare l'impostazione ***Contrassegna messaggio come spam se il conteggio è***

maggiore di digitando il valore oppure spostando il dispositivo di scorrimento verso sinistra o verso destra (*l'intervallo di valori è compreso tra 50 e 90*).

Si consiglia in genere di impostare la soglia tra 50 e 90 oppure, se non si è sicuri, su 90. Di seguito viene fornita una panoramica generale della soglia di conteggio:

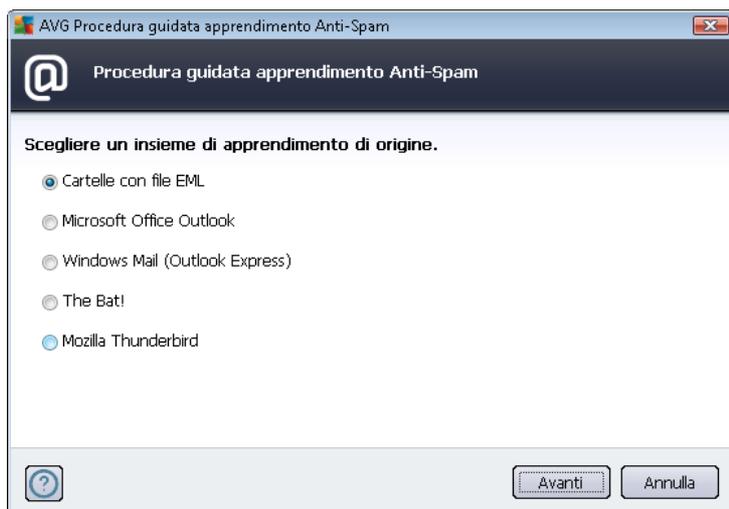
- ***Valore compreso tra 80 e 90***: verranno filtrati i messaggi e-mail il cui contenuto è probabilmente spam, ma potrebbero essere filtrati anche alcuni messaggi che non ne contengono.
- ***Valore compreso tra 60 e 79***: è considerata una configurazione piuttosto aggressiva. Verranno filtrati i messaggi e-mail il cui contenuto potrebbe essere spam, ma potrebbero essere filtrati anche messaggi che non ne contengono.
- ***Valore compreso tra 50 e 59***: configurazione particolarmente aggressiva. È probabile che insieme ai messaggi e-mail contenenti spam vengano filtrati anche i messaggi normali. Questo intervallo di valori non è consigliato per l'uso normale.

Nella finestra di dialogo delle ***impostazioni Anti-Spam*** è possibile definire ulteriormente la modalità di gestione dei messaggi e-mail di spam:

- ***Sposta messaggio nella cartella della posta indesiderata****(solo plug-in Microsoft Outlook)* : selezionare questa casella di controllo per specificare che ciascun messaggio di spam rilevato deve essere automaticamente spostato nella cartella specifica della posta indesiderata all'interno del client e-mail Microsoft Outlook. Al momento, questa funzione non è supportata in altri client e-mail.
- ***Aggiungi destinatari delle e-mail inviate alla whitelist***: selezionare questa casella di controllo per confermare che tutti i destinatari delle e-mail inviate sono affidabili e tutte le e-mail provenienti dai relativi account e-mail possono essere recapitate.
- ***Modifica oggetto per messaggi contrassegnati come spam***: selezionare questa casella di controllo se si desidera che tutti i messaggi rilevati come spam vengano contrassegnati con una parola o un carattere specifico nel campo dell'oggetto del messaggio e-mail; il testo desiderato può essere digitato nel campo di testo attivato.
- ***Chiedi conferma prima di segnalare rilevamenti errati***: se durante il processo di installazione si è scelto di partecipare al Programma di miglioramento del prodotto, si è acconsentito a segnalare le minacce rilevate a AVG. La segnalazione viene effettuata automaticamente. È tuttavia possibile selezionare questa casella di controllo per specificare se si desidera che venga richiesta una conferma prima della segnalazione ad AVG dell'eventuale spam rilevato, in modo da assicurarsi che il messaggio debba effettivamente essere classificato come spam.

Pulsanti di controllo

Il pulsante Apprendimento Anti-Spam consente di aprire la Procedura guidata apprendimento anti-spam descritta dettagliatamente nel capitolo successivo.

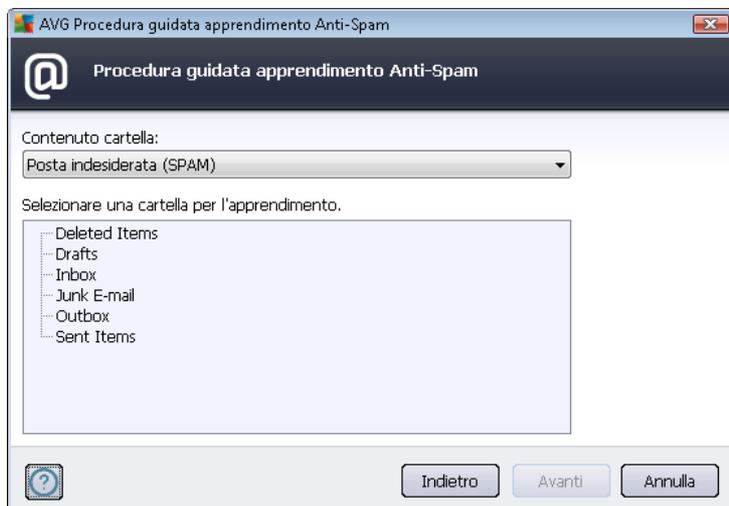
Nella prima finestra di dialogo della ***Procedura guidata apprendimento anti-spam*** viene richiesto di selezionare l'origine dei messaggi e-mail da utilizzare per l'apprendimento. Di norma, si utilizzeranno messaggi e-mail erroneamente contrassegnati come SPAM o messaggi di spam che non sono stati riconosciuti.

Sono disponibili le seguenti opzioni:

- ***Un client e-mail specifico***: se si utilizza uno dei client e-mail elencati (*MS Outlook, Outlook Express, The Bat!*), selezionare la relativa opzione
- ***Cartella con file EML***: se si utilizza qualsiasi altro programma e-mail, è necessario salvare i messaggi in una cartella specifica (*in formato .eml*) oppure accertarsi di conoscere il percorso delle cartelle dei messaggi del client e-mail. Quindi, selezionare ***Cartella con file EML***, che consentirà di individuare la cartella desiderata al passaggio successivo

Per un processo di apprendimento più semplice e rapido, è innanzitutto consigliabile ordinare i messaggi e-mail nelle cartelle, in modo che la cartella utilizzata per l'apprendimento contenga solo i messaggi per l'apprendimento (desiderati o indesiderati). Questa operazione non è tuttavia indispensabile, poiché sarà possibile filtrare i messaggi e-mail in seguito.

Selezionare l'opzione appropriata e fare clic su ***Avanti*** per continuare la procedura guidata.

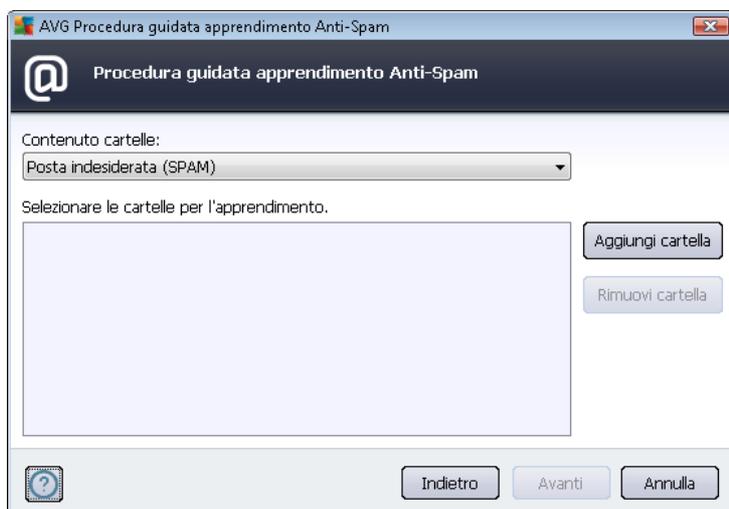
La finestra di dialogo visualizzata in questo passaggio dipende dalla selezione precedente.

Cartelle con file EML

In questa finestra di dialogo selezionare la cartella contenente i messaggi che si desidera utilizzare per l'apprendimento. Fare clic sul pulsante ***Aggiungi cartella*** per individuare la cartella con i file .eml (*messaggi e-mail salvati*). La cartella selezionata verrà visualizzata nella finestra di dialogo.

Nel menu a discesa ***Contenuto delle cartelle*** impostare una delle due opzioni per indicare se la cartella selezionata contiene posta desiderata (*HAM*) o indesiderata (*SPAM*). Notare che al passaggio successivo sarà possibile filtrare i messaggi, pertanto non è necessario che la cartella contenga soltanto i messaggi necessari per l'apprendimento. È inoltre possibile rimuovere le cartelle indesiderate selezionate dall'elenco facendo clic sul pulsante ***Rimuovi cartella***.

Una volta eseguita l'operazione, fare clic su ***Avanti*** e passare a Opzioni di filtro dei messaggi.

Client e-mail specifico

Dopo aver confermato un'opzione, viene visualizzata una nuova finestra di dialogo.

Nota: *se si utilizza Microsoft Outlook, verrà richiesto innanzitutto di selezionare il profilo di MS Outlook.*

Nel menu a discesa ***Contenuto delle cartelle*** impostare una delle due opzioni per indicare se la cartella selezionata contiene posta desiderata (*HAM*) o indesiderata (*SPAM*). Notare che al passaggio successivo sarà possibile filtrare i messaggi, pertanto non è necessario che la cartella contenga soltanto i messaggi necessari per l'apprendimento. Nella sezione principale della finestra di dialogo è già visualizzata una struttura di esplorazione del client e-mail selezionato. Individuare la cartella desiderata nella struttura ed evidenziarla utilizzando il mouse.

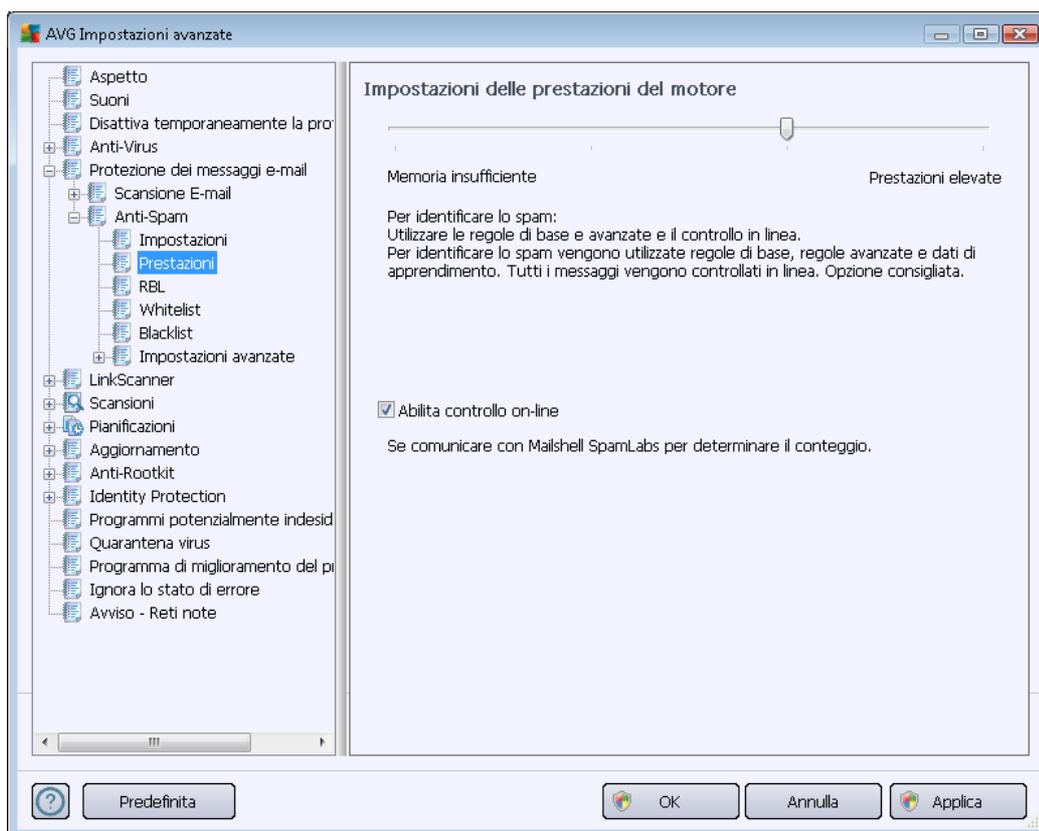
Una volta eseguita l'operazione, fare clic su ***Avanti*** e passare a Opzioni di filtro dei messaggi.

In questa finestra di dialogo è possibile impostare il filtro per i messaggi e-mail.

- ***Tutti i messaggi (nessun filtro)***: se si è certi che la cartella selezionata contiene soltanto messaggi che si desidera utilizzare per l'apprendimento, selezionare l'opzione ***Tutti i messaggi (nessun filtro)***.
- ***Usa filtro***: per le opzioni di filtro avanzate, selezionare l'opzione ***Usa filtro***. È possibile inserire una parola (*nome*), una parte di una parola o una frase da ricercare nell'oggetto dell'e-mail e/o nel campo del mittente. Tutti i messaggi che corrispondono esattamente ai criteri specificati verranno utilizzati per l'apprendimento, senza che vengano visualizzate ulteriori richieste di conferma. Se si compilano entrambi i campi di testo, verranno utilizzati anche gli indirizzi che corrispondono a uno solo dei criteri.
- ***Chiedi per ogni messaggio***: se non si è certi dei messaggi contenuti nella cartella e si desidera che durante la procedura guidata venga richiesta una conferma per ogni singolo messaggio *(al fine di determinare se utilizzarlo o meno per l'apprendimento)*, selezionare l'opzione ***Chiedi per ogni messaggio***.

Dopo aver selezionato l'opzione appropriata, fare clic su ***Avanti***. La finestra di dialogo seguente avrà uno scopo puramente informativo, in quanto indica che la procedura guidata è pronta per l'elaborazione dei messaggi. Per avviare l'apprendimento, fare nuovamente clic su ***Avanti***.

L'apprendimento viene avviato in base alle condizioni precedentemente selezionate.

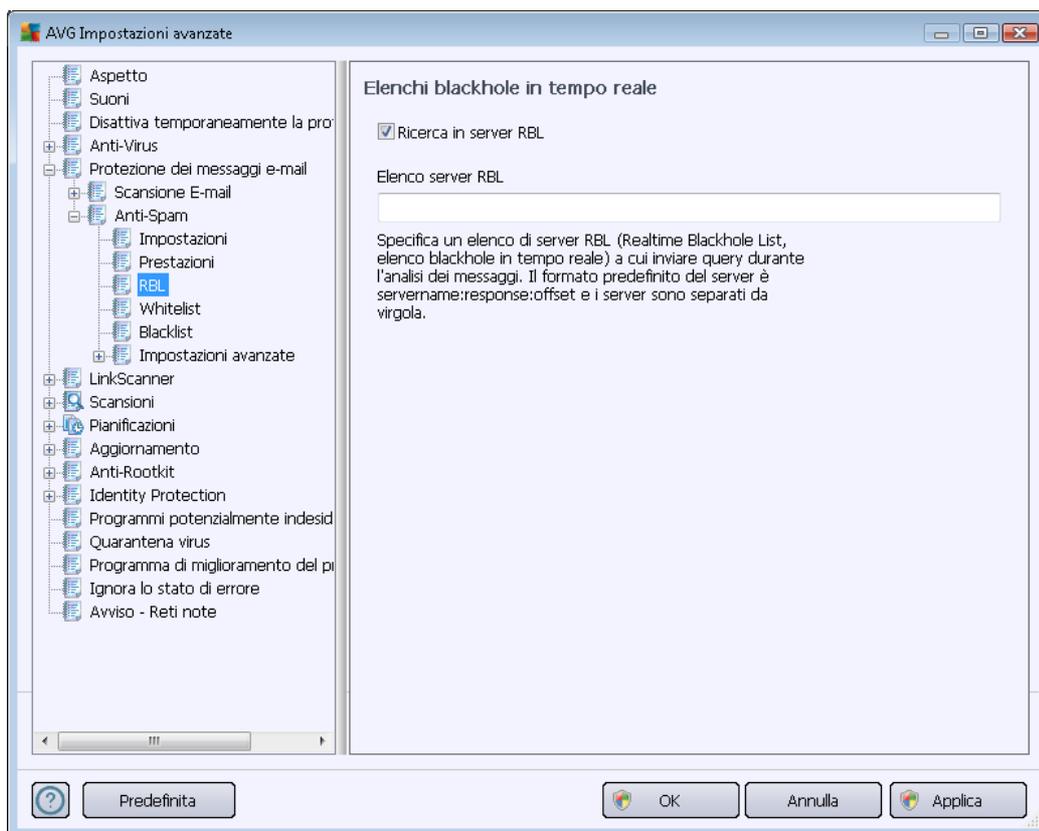
La finestra di dialogo ***Impostazioni delle prestazioni del motore*** (*accessibile dalla voce **Prestazioni** della struttura di esplorazione visualizzata a sinistra*) include le impostazioni delle prestazioni del componente ***Anti-Spam:***

Spostare il dispositivo di scorrimento a sinistra o a destra per modificare il livello dell'intervallo delle prestazioni di scansione tra le modalità ***Memoria insufficiente*** / ***Prestazioni elevate***.

- ***Memoria insufficiente***: durante il processo di scansione per l'identificazione dello spam, non viene utilizzata alcuna regola. Per l'identificazione dello spam verranno utilizzati solo i dati di formazione. Questa modalità non è consigliata, a meno che l'hardware del computer non sia estremamente limitato.

- ***Prestazioni elevate***: questa modalità richiederà una notevole quantità di memoria. Durante il processo di scansione per l'identificazione dello spam verranno utilizzate le seguenti funzionalità: regole e cache del database di spam, regole di base e avanzate, indirizzi IP e database di spammer.

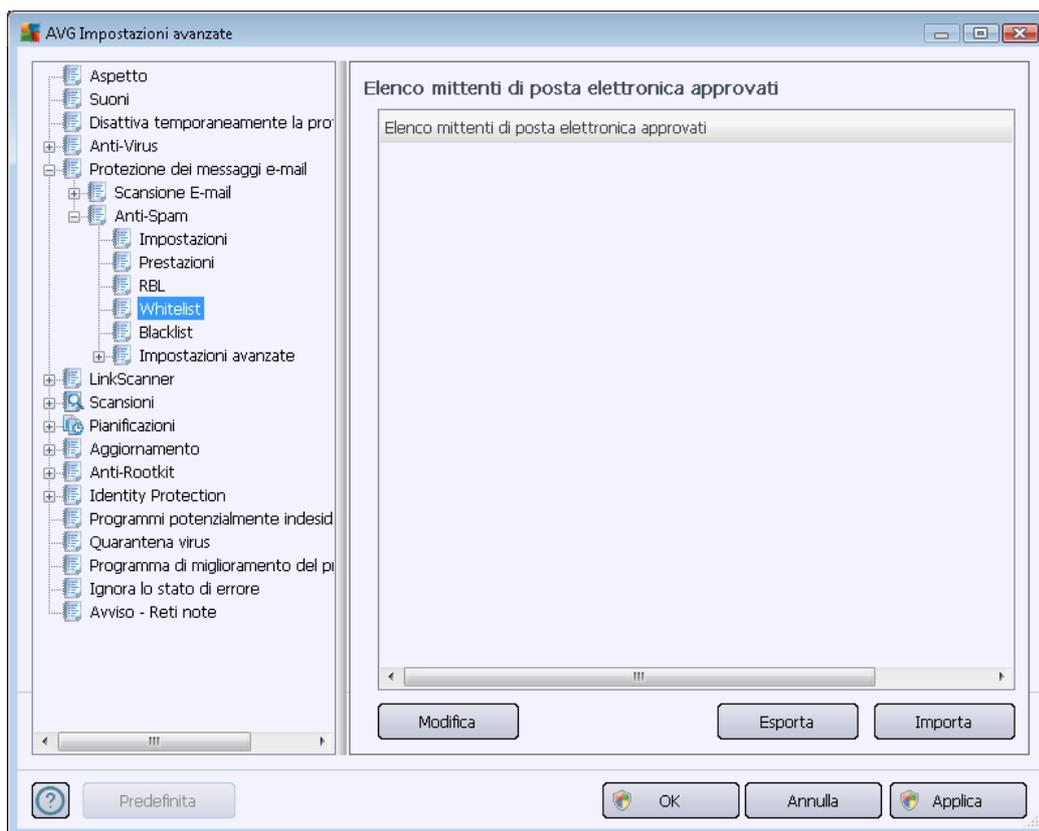
La voce ***Abilita controllo on-line*** è attiva per impostazione predefinita. Ne risulta un rilevamento dello spam più preciso tramite la comunicazione con i server Mailshell, ovvero i dati sottoposti a scansione verranno confrontati con i database Mailshell in linea.

In genere si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo. Le eventuali modifiche alla configurazione devono essere eseguite solo da utenti esperti.

La voce **RBL** apre una finestra di dialogo di modifica denominata ***Elenchi blackhole in tempo reale*** in cui è possibile attivare/disattivare la funzione ***Ricerca in server RBL***:

Il server RBL (*Realtime Blackhole List, Elenchi blackhole in tempo reale*) è un server DNS con un vasto database di mittenti di spam noti. Se questa funzione è attivata, tutti i messaggi e-mail verranno verificati in base al database del server RBL e verranno contrassegnati come spam se risulteranno identici a una delle voci presenti nel database. I database dei server RBL contengono le impronte digitali di spam più aggiornate, per fornire il rilevamento migliore e più accurato. La funzione è particolarmente utile per gli utenti che ricevono grandi quantità di messaggi di spam normalmente non rilevati dal motore Anti-Spam.

L'***elenco dei server RBL*** consente di definire specifiche posizioni per i server RBL (*l'attivazione di questa funzionalità potrebbe rallentare il processo di ricezione dei messaggi e-mail in alcuni sistemi e configurazioni, poiché ogni singolo messaggio deve essere confrontato con il database del server RBL).*

Non vengono inviati dati personali al server.

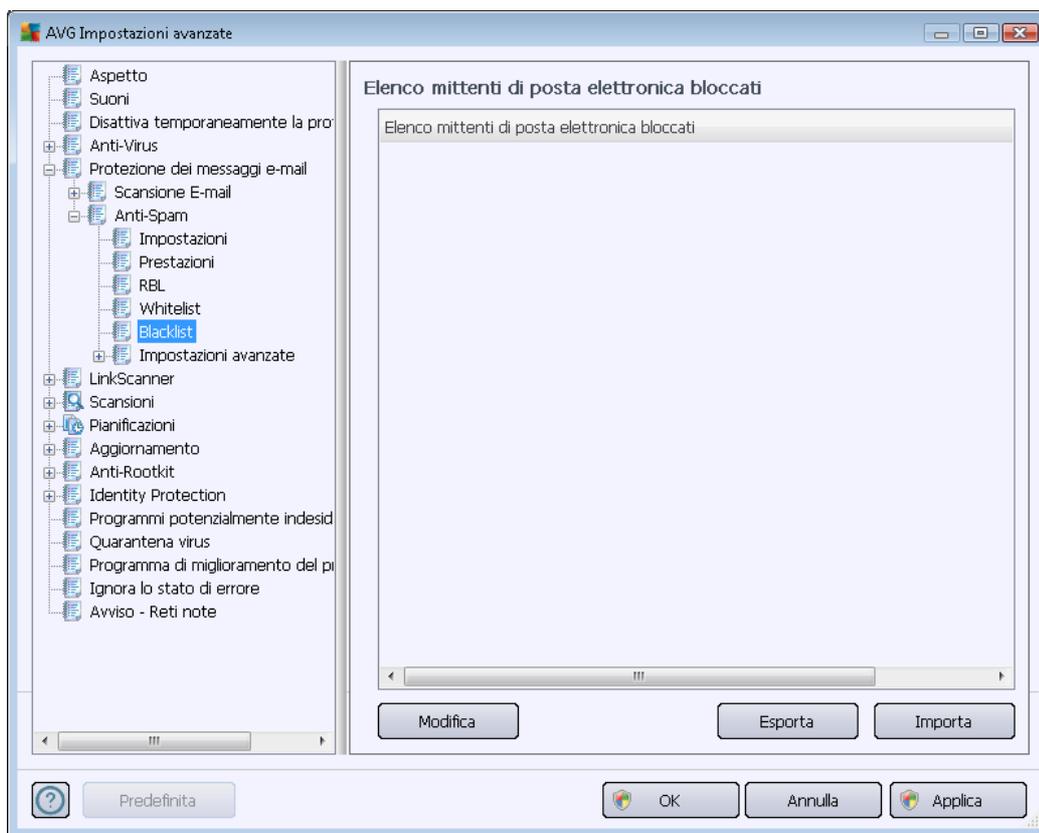
La voce ***Whitelist*** consente di aprire la finestra di dialogo ***Elenco mittenti di posta elettronica approvati*** con un elenco globale di nomi di dominio e indirizzi e-mail approvati i cui messaggi non verranno mai contrassegnati come spam.

Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza che non verranno mai inviati messaggi indesiderati (spam). È inoltre possibile compilare un elenco di nomi di dominio completi (*ad esempio avg.com*) che non generano mai messaggi spam. Dopo che è stato preparato l'elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: immettendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi.

Pulsanti di controllo

Sono disponibili i seguenti pulsanti di controllo:

- ***Modifica***: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile immettere manualmente un elenco di indirizzi (*è inoltre possibile utilizzare il metodo copia e incolla*). Immettere una voce (*mittente o nome di dominio*) per riga.
- ***Esporta***: se per qualsiasi motivo si decide di esportare i record, è possibile fare clic su questo pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante. Il file deve includere una sola voce (*indirizzo, nome di dominio*) per riga.

La voce ***Blacklist*** consente di aprire una finestra di dialogo contenente un elenco globale di nomi di dominio e indirizzi e-mail di mittenti bloccati i cui messaggi saranno sempre contrassegnati come spam.

Nell'interfaccia di modifica è possibile compilare un elenco di mittenti da cui si ha la certezza di ricevere messaggi indesiderati *(spam)*. È inoltre possibile compilare un elenco di nomi di dominio completi (*ad esempio aziendaspam.com*) da cui si prevede di ricevere o si ricevono messaggi di spam. Tutti i messaggi e-mail ricevuti da tali indirizzi o domini specifici verranno contrassegnati come spam. Dopo che è stato preparato l'elenco di mittenti e/o nomi di dominio, è possibile inserirli in due modi diversi: immettendo direttamente ciascun indirizzo e-mail o importando tutto l'elenco di indirizzi.

Pulsanti di controllo

Sono disponibili i seguenti pulsanti di controllo:

- ***Modifica***: selezionare questo pulsante per aprire una finestra di dialogo in cui è possibile

immettere manualmente un elenco di indirizzi (*è inoltre possibile utilizzare il metodo copia e incolla*). Immettere una voce (*mittente o nome di dominio*) per riga.

- ***Esporta***: se per qualsiasi motivo si decide di esportare i record, è possibile fare clic su questo pulsante per eseguire l'operazione. Tutti i record verranno salvati in un file di testo normale.

- ***Importa***: se si possiede già un file di testo di indirizzi di posta elettronica o nomi di dominio, è possibile importare tale file selezionando questo pulsante.

Il ramo Impostazioni avanzate contiene opzioni complete di impostazione per il componente Anti-Spam. Queste impostazioni sono destinate esclusivamente agli utenti esperti, in particolare agli amministratori di rete che devono eseguire una configurare dettagliata della protezione anti-spam per garantire la massima protezione dei server e-mail. Per questo motivo non è disponibile una guida aggiuntiva nelle singole finestre di dialogo. Tuttavia, è disponibile direttamente nell'interfaccia utente una breve descrizione di ciascuna opzione.

Si consiglia di non modificare alcuna impostazione a meno che non si disponga di una conoscenza approfondita delle impostazioni avanzate di Spamcatcher (MailShell Inc.). Eventuali modifiche inappropriate possono dare luogo a una riduzione delle prestazioni o a un funzionamento errato del componente.

Se si ritiene di dover modificare comunque la configurazione di Anti-Spam a un livello molto avanzato, seguire le istruzioni fornite direttamente nell'interfaccia utente. In genere, in ciascuna finestra di dialogo è contenuta una sola funzionalità specifica che può essere modificata. La descrizione relativa è sempre inclusa nella finestra di dialogo:

- ***Cache***: impronte digitali, reputazione dominio, LegitRepute

- ***Apprendimento***: numero massimo di parole, soglia di apprendimento automatico, peso

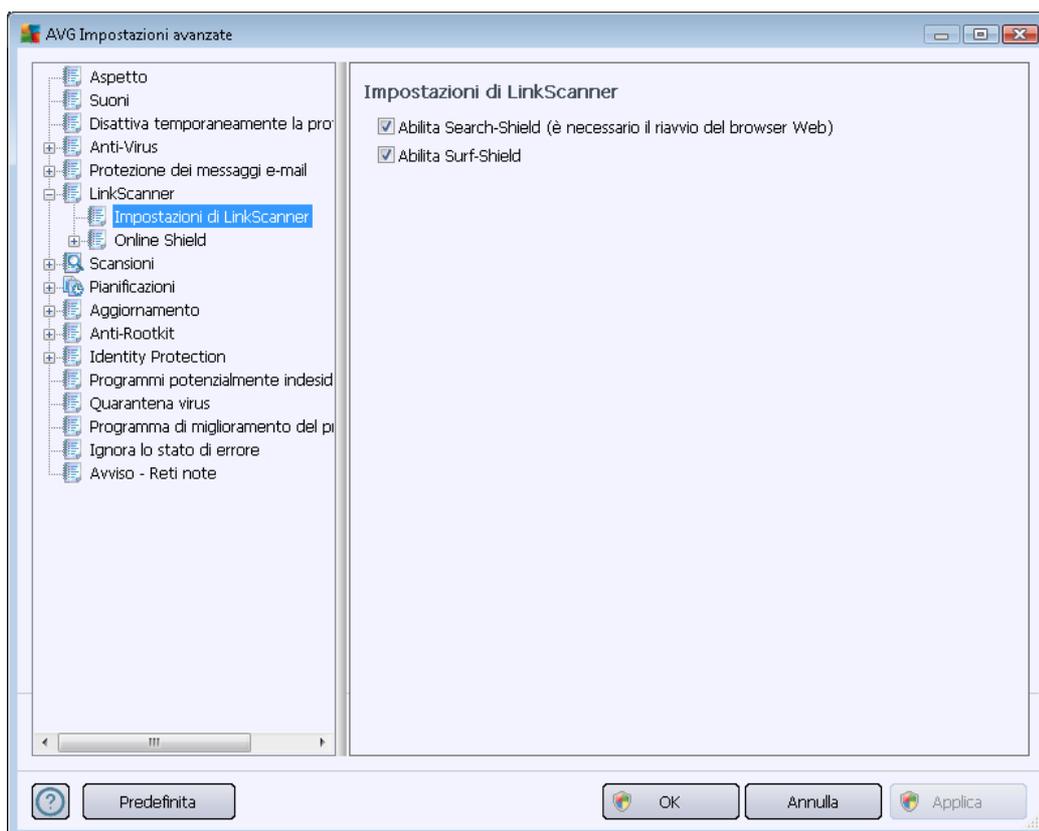
- ***Filtraggio***: elenco lingue, elenco paesi, IP approvati, IP bloccati, paesi bloccati, set di caratteri bloccati, mittenti contraffatti

- ***RBL***: server RBL, multihit, soglia, timeout, IP massimi

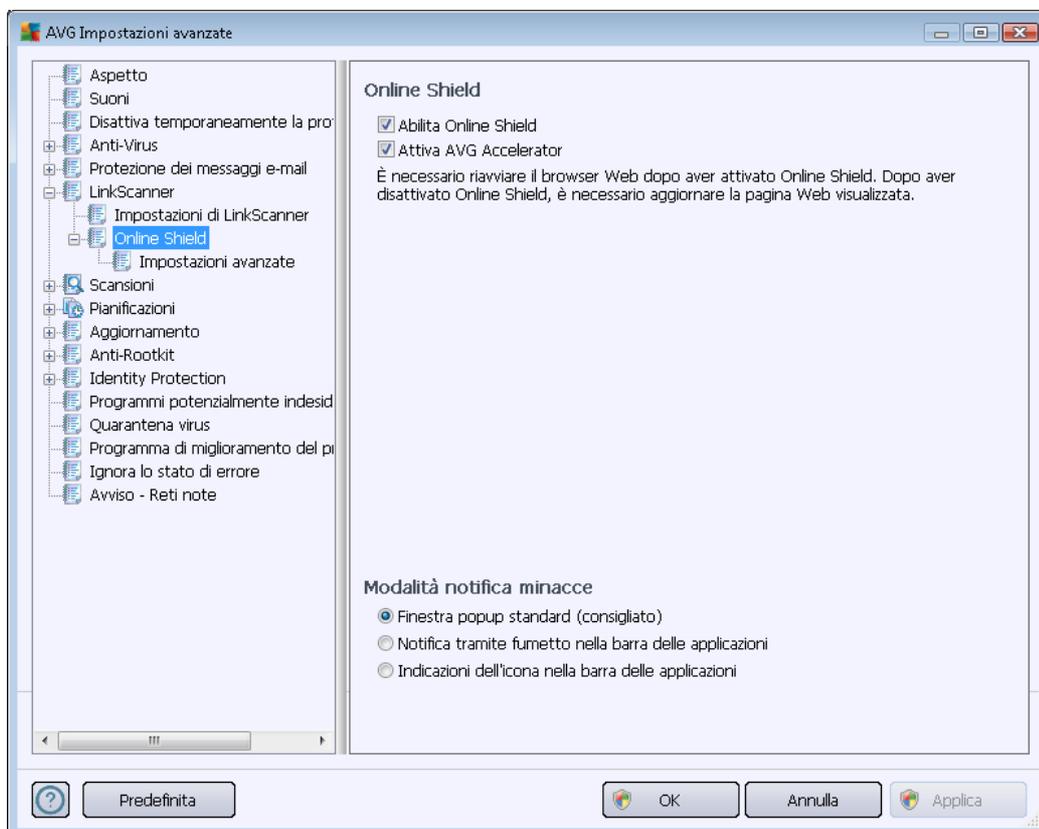
- ***Connessione Internet***: timeout, server proxy, autenticazione proxy

10.6. LinkScanner

10.6.1. Impostazioni LinkScanner

La finestra di dialogo ***Impostazioni LinkScanner*** consente di attivare/disattivare le funzionalità di base del componente LinkScanner:

- ***Abilita Search-Shield*** (*attivata per impostazione predefinita*): icone informative relative ai siti restituiti dalle ricerche eseguite in Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg o SlashDot il cui contenuto è stato precedentemente controllato.

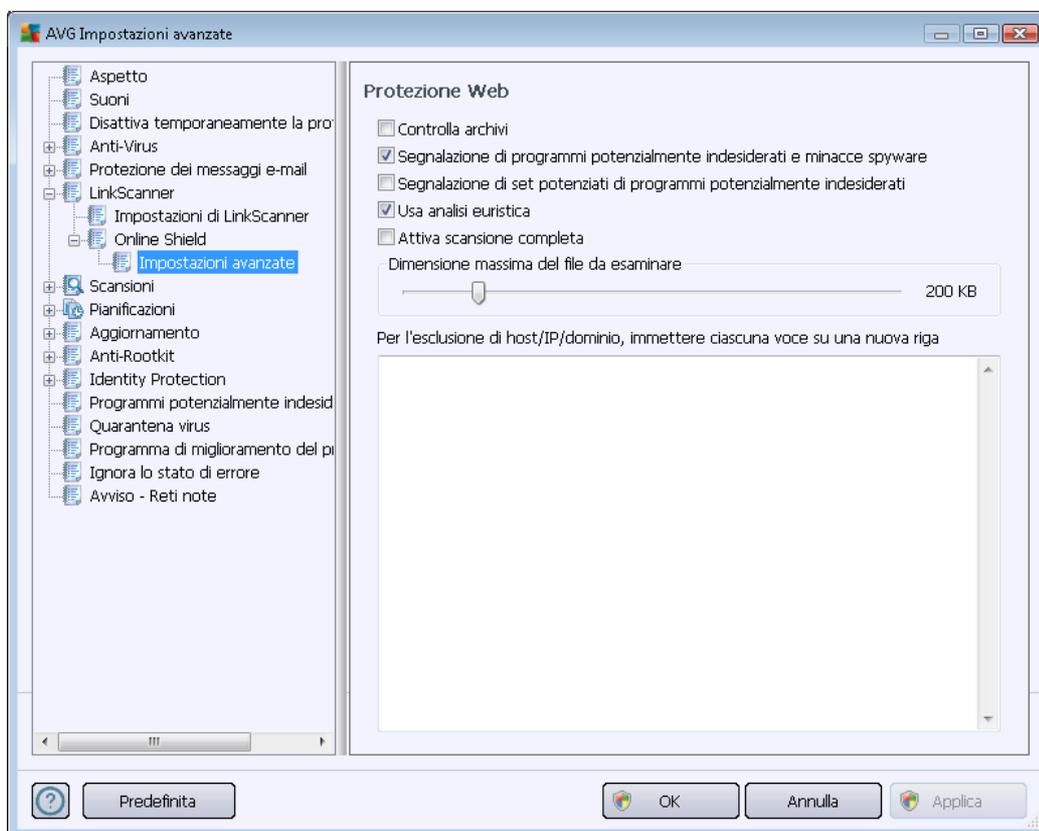
- ***Abilita Surf-Shield***: (*attivata per impostazione predefinita*) protezione attiva (*in tempo reale*) da siti dannosi al momento dell'accesso. Le connessioni a siti dannosi noti e il loro contenuto vengono bloccati non appena l'utente esegue l'accesso mediante un browser Web (*o qualsiasi altra applicazione che utilizza HTTP*).

10.6.2. Online Shield

La finestra di dialogo ***Online Shield*** offre le seguenti opzioni:

- ***Abilita Online Shield*** *(attivata per impostazione predefinita)*: attiva/disattiva l'intero servizio ***Online Shield***. Per ulteriori impostazioni avanzate di ***Online Shield***, passare alla successiva finestra di dialogo denominata Protezione Web.

- ***Attiva AVG Accelerator*** *(attivata per impostazione predefinita):* attiva/disattiva il servizio ***AVG Accelerator*** che ottimizza la riproduzione dei video in linea e semplifica il download.

Modalità notifica minacce

Nella parte inferiore della finestra di dialogo, scegliere in che modo si desidera essere informati circa eventuali minacce rilevate: mediante una finestra popup standard, mediante una notifica tramite fumetto nella barra delle applicazioni oppure mediante le informazioni dell'icona nella barra delle applicazioni.

La finestra di dialogo ***Protezione Web*** consente di modificare la configurazione del componente relativamente alla scansione del contenuto di siti Web. L'interfaccia di modifica consente di configurare le seguenti opzioni di base:

- ***Abilita protezione Web***: questa opzione conferma l'esecuzione della scansione del contenuto delle pagine Web da parte del componente ***Online Shield***. Se questa opzione è attiva (*per impostazione predefinita*), è possibile attivare/disattivare le voci seguenti:
    - ***Controlla archivi*** (*disattivata per impostazione predefinita*): consente di eseguire la scansione del contenuto di eventuali archivi inclusi nella pagina Web da visualizzare.
    - ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
    - ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi

successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Usa analisi euristica*** (*attivata per impostazione predefinita*): consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo dell'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Dimensione massima del file da esaminare***: se i file inclusi sono presenti nella pagina visualizzata, è inoltre possibile eseguire la scansione del relativo contenuto prima che questi vengano scaricati nel computer. Tuttavia, la scansione di file di grandi dimensioni richiede parecchio tempo rallentando notevolmente il download della pagina Web. È possibile utilizzare la barra di scorrimento per specificare la dimensione massima di un file che deve ancora essere sottoposto a scansione da ***Online Shield***. Anche se le dimensioni del file scaricato sono superiori a quelle specificate, quindi il file non verrà sottoposto a scansione da Online Shield, il computer è comunque protetto: se il file fosse infetto, verrebbe rilevato immediatamente da ***Resident Shield***.

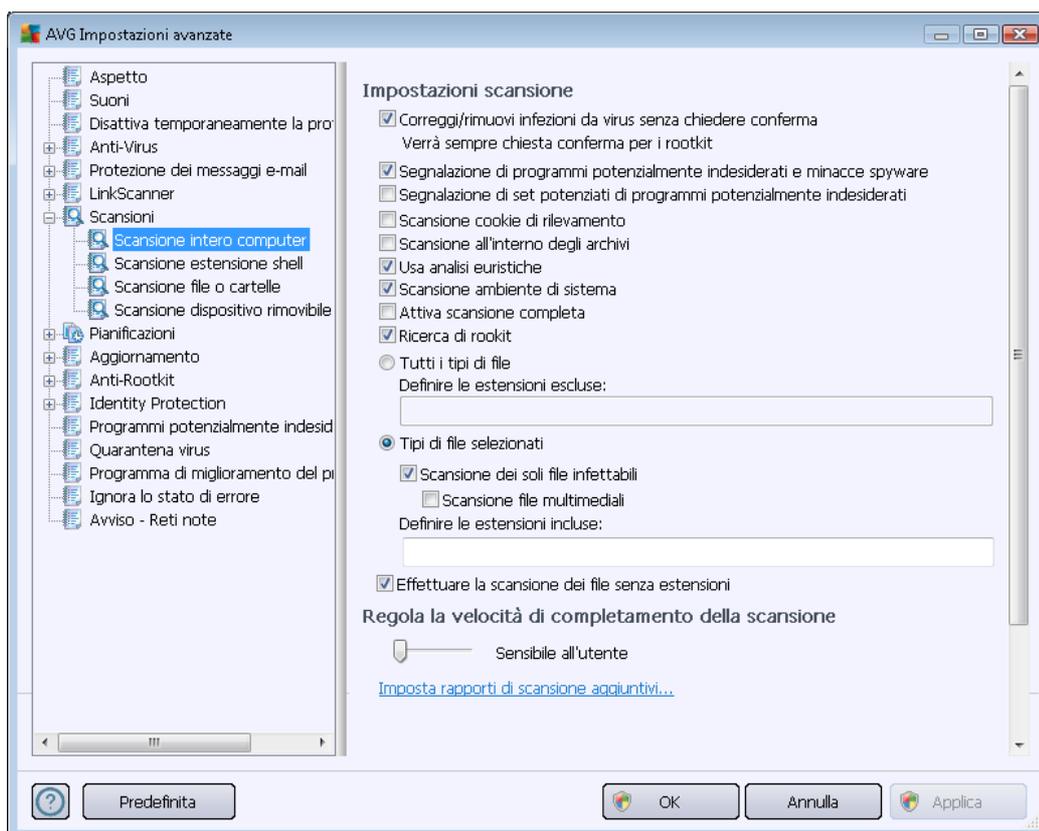
- ***Escludi host/IP/dominio***: nel campo è possibile digitare il nome esatto di un server (*host, indirizzo IP, indirizzo IP con maschera o URL*) o un dominio che non deve essere sottoposto a scansione da ***Online Shield***. Pertanto, escludere un host solo se si è assolutamente certi che non fornirà mai contenuti Web pericolosi.

10.7. Scansioni

La sezione delle impostazioni di scansione avanzate è suddivisa in quattro categorie che fanno riferimento a specifici tipi di scansione definiti dal fornitore del software:

- ***Scansione intero computer***: scansione predefinita standard dell'intero computer
- ***Scansione estensione shell***: scansione specifica di un oggetto selezionato direttamente dall'ambiente Esplora risorse
- ***Scansione file o cartelle***: scansione predefinita standard di aree selezionate del computer
- ***Scansione dispositivo rimovibile***: scansione specifica di dispositivi rimovibili collegati al computer

10.7.1. Scansione intero computer

L'opzione ***Scansione intero computer*** consente di modificare i parametri di una delle scansioni predefinite dal fornitore del software, ossia Scansione intero computer:

Impostazioni scansione

Nella sezione ***Impostazioni scansione*** è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati a seconda delle necessità:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** (*attivata per impostazione predefinita*): se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.
- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro del componente Anti-Spyware stabilisce che i cookie devono essere rilevati (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*)

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche quelli inclusi all'interno di un archivio, quale ZIP, RAR e così via

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rookit*** (*attivata per impostazione predefinita*): la scansione Anti-Rootkit cerca nel computer possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Quindi è necessario decidere se si desidera sottoporre a scansione:

- ***Tutti i tipi di file***: è possibile definire eccezioni fornendo un elenco di estensioni di file separate da virgola (*dopo il salvataggio, le virgole si trasformano in punto e virgola*) da non sottoporre a scansione;

- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

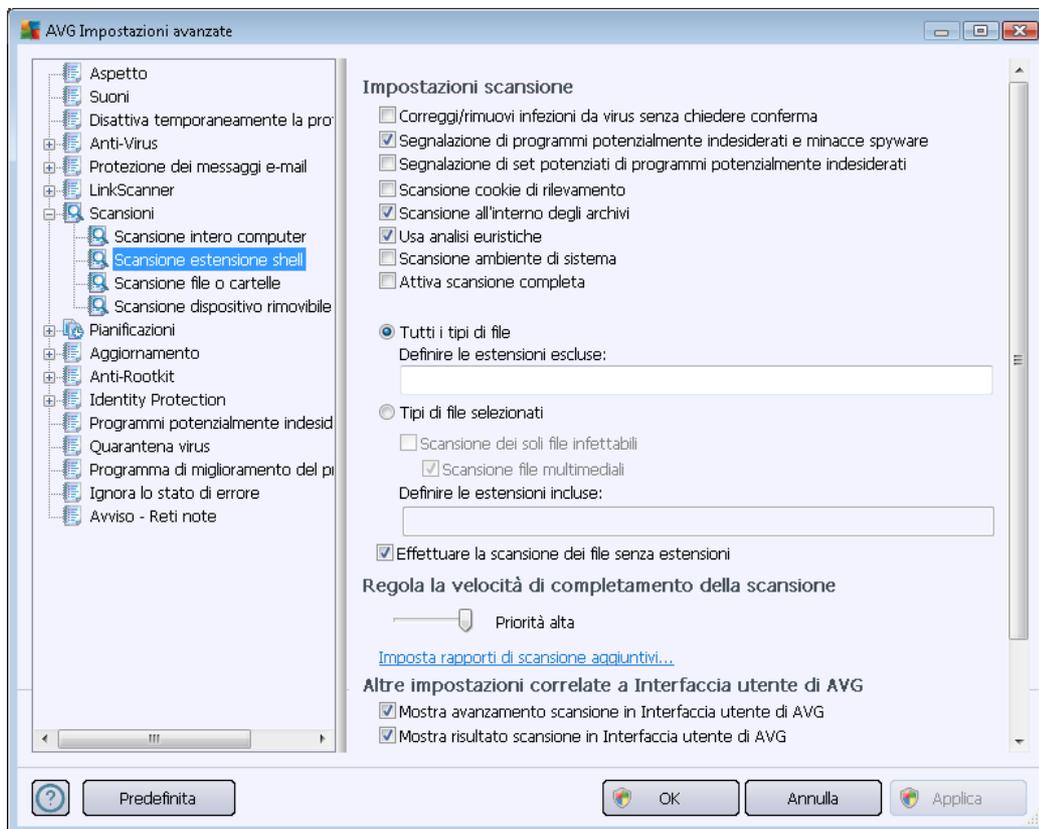
Regola la velocità di completamento della scansione

All'interno della sezione ***Regola la velocità di completamento della scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

Imposta rapporti di scansione aggiuntivi...

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

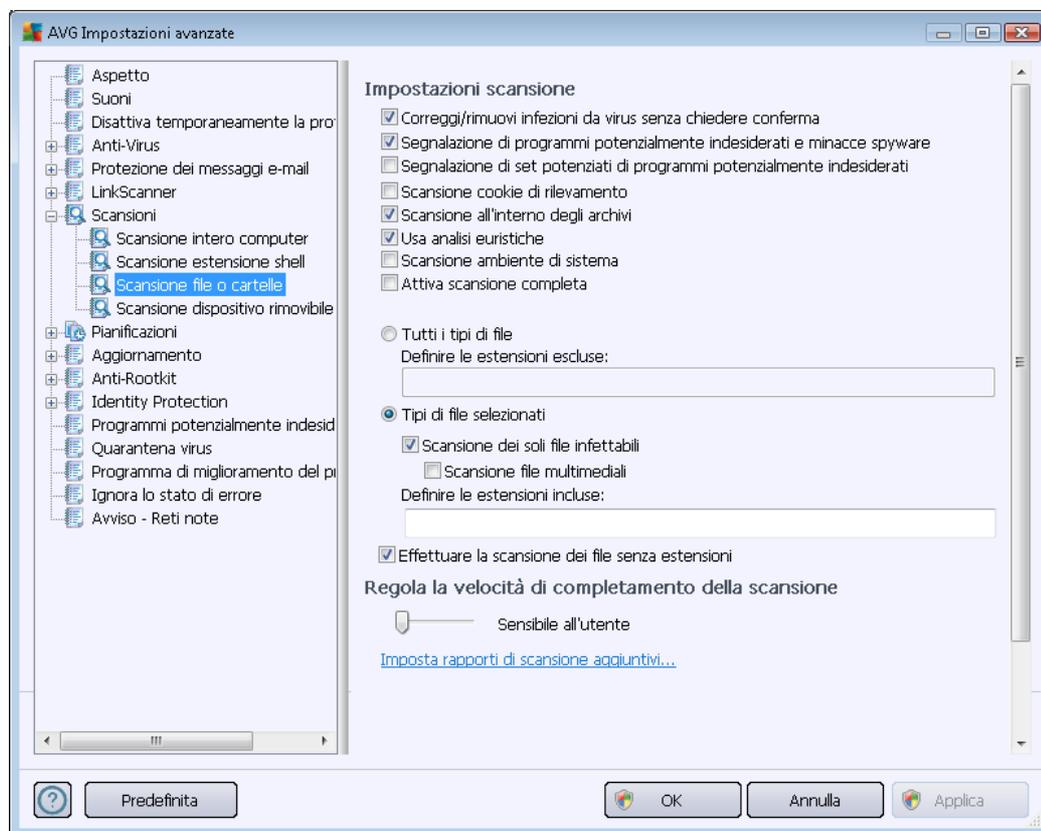
10.7.2. Scansione estensione shell

Simile alla voce precedente denominata Scansione intero computer, ***Scansione estensione shell*** offre anche numerose opzioni per modificare la scansione predefinita dal fornitore del software. In questo caso, la configurazione è relativa alla scansione di oggetti specifici avviati direttamente dall'ambiente Esplora risorse (*estensione shell*), vedere il capitolo Scansione in Esplora risorse:

L'elenco dei parametri è identico a quello disponibile per Scansione intero computer. Tuttavia, le impostazioni predefinite sono diverse (*ad esempio, per impostazione predefinita Scansione intero computer non controlla gli archivi ma esamina l'ambiente di sistema, viceversa per Scansione estensione shell*).

Nota: *per la descrizione di parametri specifici consultare il capitolo Impostazioni AVG avanzate / Scansione / Scansione intero computer.*

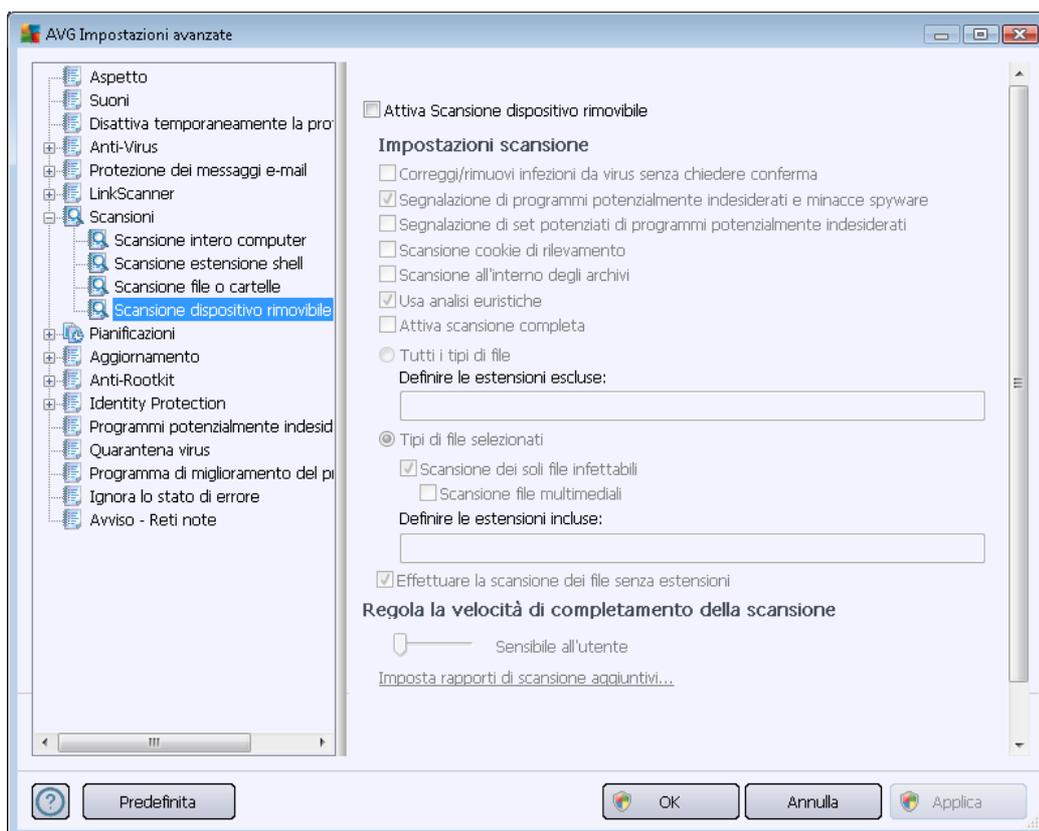
Rispetto alla finestra di dialogo Scansione intero computer, la finestra di dialogo ***Scansione estensione shell*** include inoltre la sezione denominata ***Altre impostazioni correlate all'Interfaccia utente di AVG***, in cui è possibile specificare se si desidera accedere all'avanzamento della scansione e ai risultati della scansione dall'Interfaccia utente di AVG. Inoltre, è possibile definire se il risultato della scansione deve essere visualizzato solo nel caso in cui venga rilevata un'infezione durante la scansione.

10.7.3. Scansione file o cartelle

L'interfaccia di modifica di ***Scansione file o cartelle*** è identica alla finestra di dialogo di modifica Scansione intero computer. Tutte le opzioni di configurazione sono uguali; tuttavia, le impostazioni predefinite sono più restrittive per Scansione intero computer:

Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con il comando Scansione file o cartelle!

Nota: *per la descrizione di parametri specifici consultare il capitolo Impostazioni AVG avanzate / Scansione / Scansione intero computer.*

10.7.4. Scansione dispositivo rimovibile

L'interfaccia di modifica di ***Scansione dispositivo rimovibile*** è inoltre molto simile alla finestra di dialogo di modifica Scansione intero computer:

La ***Scansione dispositivo rimovibile*** viene avviata automaticamente quando viene collegato un dispositivo rimovibile al computer. Per impostazione predefinita, questa scansione è disattivata. Tuttavia, è molto importante effettuare la scansione dei dispositivi rimovibili per verificare la presenza di potenziali minacce poiché tali dispositivi rappresentano una delle fonti di infezione principali. Per avviare automaticamente questo tipo di scansione quando necessario, selezionare l'opzione ***Abilita scansione dispositivo rimovibile***.

Nota: *per la descrizione di parametri specifici consultare il capitolo Impostazioni AVG avanzate / Scansione / Scansione intero computer.*

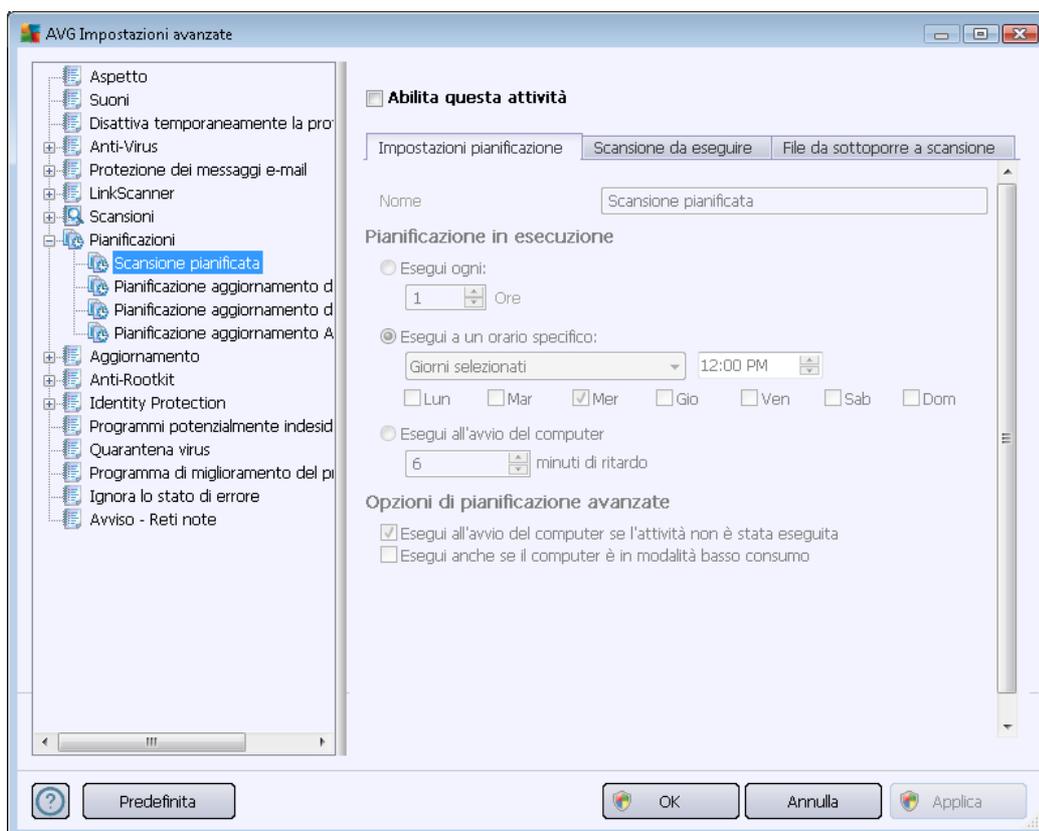
10.8. Pianificazioni

Nella sezione ***Pianificazioni*** è possibile modificare le impostazioni predefinite di:

- Scansione pianificata
- Pianificazione aggiornamento definizioni
- Pianificazione aggiornamento del programma

- Pianificazione aggiornamenti Anti-Spam

10.8.1. Scansione pianificata

È possibile modificare i parametri della scansione pianificata (*o configurare una nuova pianificazione*) in tre schede. In ciascuna scheda è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità:

Quindi, nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma. Per le pianificazioni aggiunte successivamente (*è possibile aggiungere una nuova pianificazione facendo clic con il pulsante destro del mouse sulla voce **Scansione pianificata** nella struttura di esplorazione a sinistra*) è possibile specificare un nome personalizzato. In tal caso, il campo di testo sarà attivo per la modifica. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

Esempio: *non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via. Inoltre, non è necessario specificare nel nome della scansione se si tratta di una scansione dell'intero computer oppure relativa solo ai file o alle cartelle selezionati. Le scansioni saranno sempre una versione specifica della scansione dei file e delle cartelle selezionati.*

In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora tramite l'avvio ripetuto della scansione dopo un certo periodo di tempo (***Esegui ogni...***) oppure specificando data e ora esatte (***Esegui a determinati intervalli di tempo...***) o specificando un evento a cui dovrà essere associato l'avvio della scansione (***Esegui all'avvio del computer***).

Opzioni di pianificazione avanzate

Questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento. Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni:

Viene quindi visualizzata una nuova icona AVG nella barra delle applicazioni (*completamente colorata e con una luce lampeggiante*) per comunicare che è in corso una scansione pianificata. Fare clic con il pulsante destro del mouse sull'icona AVG della scansione in esecuzione per aprire un menu di scelta rapida in cui è possibile decidere se sospendere o arrestare la scansione in esecuzione, nonché modificarne la priorità.

Nella scheda ***Scansione da eseguire*** è presente un elenco di parametri che possono essere attivati o disattivati facoltativamente. Per impostazione predefinita, la maggior parte dei parametri è attivata e la funzionalità verrà applicata durante la scansione. ***A meno che non esista un motivo valido per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita***:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita):* se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (***attivata per impostazione predefinita***): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che

potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro del componente Anti-Spyware stabilisce che i cookie devono essere rilevati durante la scansione (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*).

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita):* in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*), per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rootkit*** *(attivata per impostazione predefinita): la scansione* Anti-Rootkit cerca nel computer possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Quindi è necessario decidere se si desidera sottoporre a scansione:

- ***Tutti i tipi di file***: è possibile definire eccezioni fornendo un elenco di estensioni di file separate da virgola (*dopo il salvataggio, le virgole si trasformano in punto e virgola*) da non sottoporre a scansione;

- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

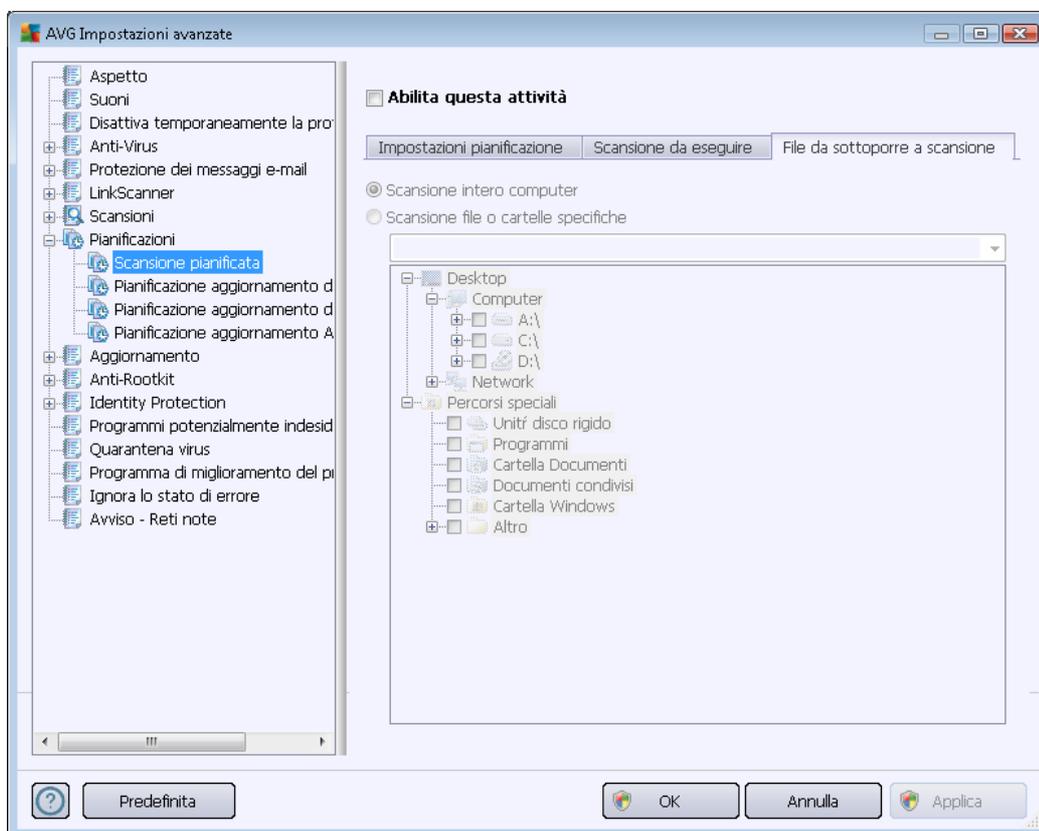
Regola la velocità di completamento della scansione

All'interno della sezione ***Regola la velocità di completamento della scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non è utilizzato*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

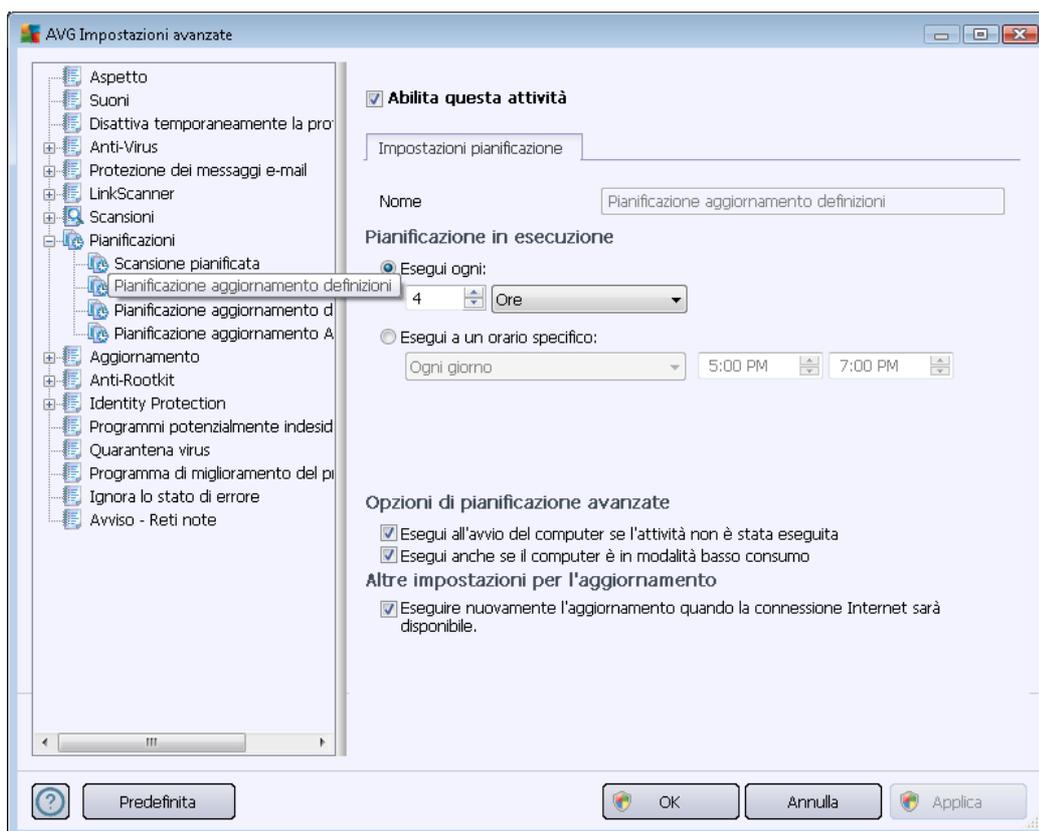
Imposta rapporti di scansione aggiuntivi

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

Impostazioni di scansione aggiuntive

Fare clic su ***Impostazioni di scansione aggiuntive...*** per aprire una nuova finestra di dialogo ***Opzioni arresto computer*** in cui è possibile decidere se il computer deve essere arrestato in modo automatico al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

Nella scheda ***File da sottoporre a scansione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle specifiche. Se si seleziona la scansione di file o cartelle specifiche, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione.

10.8.2. Pianificazione aggiornamento definizioni

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento delle definizioni pianificato e attivarlo nuovamente in seguito:

In questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento delle definizioni. Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

In questa sezione, specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento delle definizioni pianificato. L'intervallo può essere definito tramite l'avvio dell'aggiornamento ripetuto dopo un determinato periodo di tempo (***Esegui ogni...***) oppure specificando una data e un'ora esatte (***Esegui a un orario specifico...***).

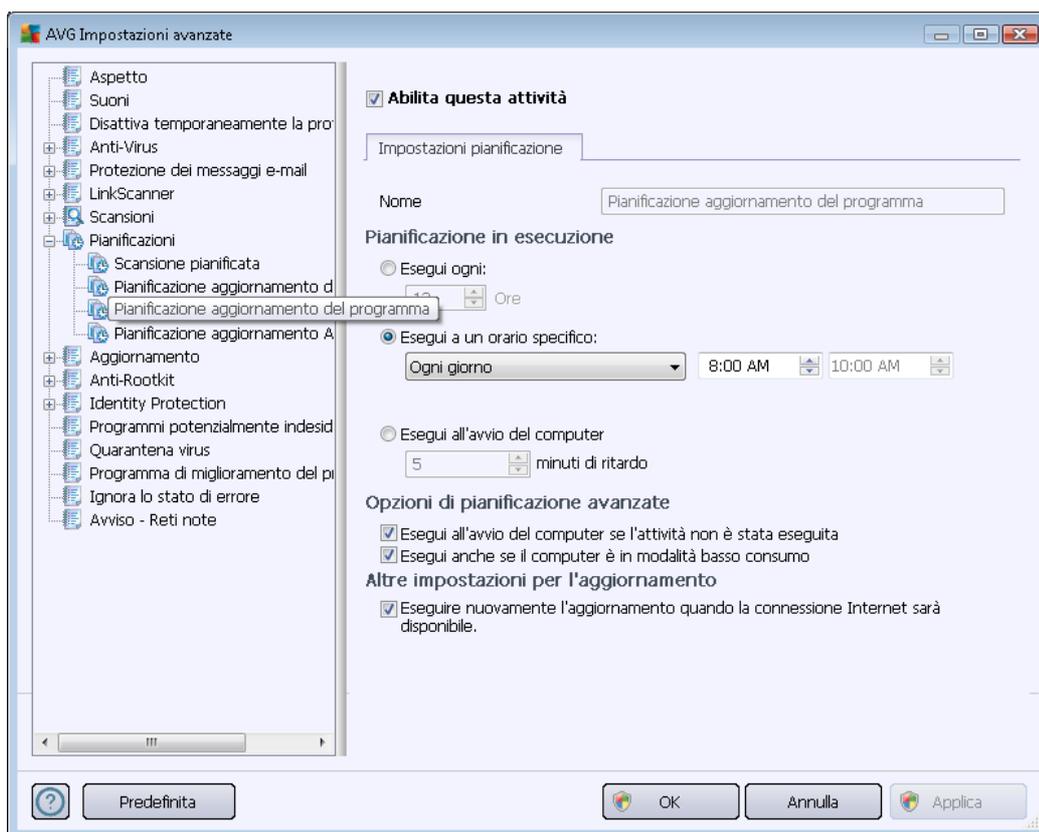
Opzioni di pianificazione avanzate

Questa sezione consente di definire le circostanze in cui deve o non deve essere avviato l'aggiornamento delle definizioni se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni di aggiornamento

Infine, selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando l'aggiornamento pianificato viene avviato in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

10.8.3. Pianificazione dell'aggiornamento del programma

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del programma pianificato e attivarlo nuovamente in seguito:

Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento del programma pianificato. È possibile definire l'ora tramite l'avvio ripetuto dell'aggiornamento dopo un certo periodo

di tempo (***Esegui ogni...***) oppure definendo data e ora esatte (***Esegui a un orario specifico...***) o definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Azione in base all'avvio del computer***).

Opzioni di pianificazione avanzate

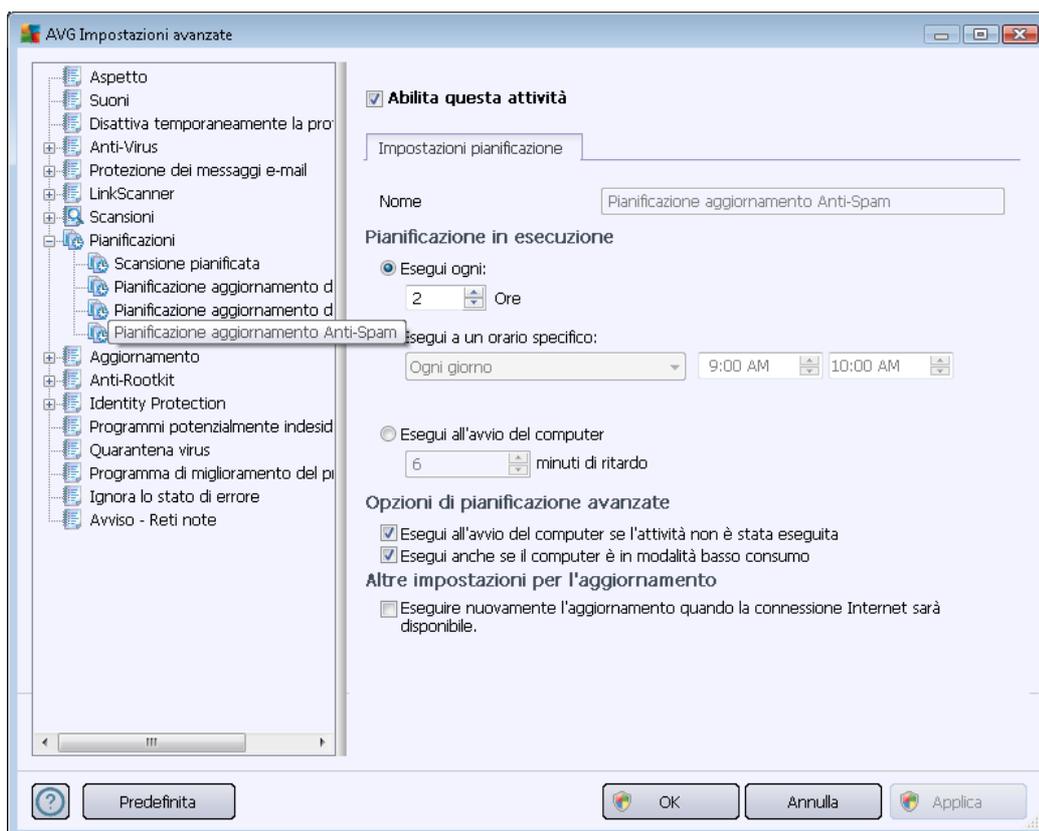
Questa sezione consente di definire le circostanze in cui deve o non deve essere avviato l'aggiornamento del programma se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni per l'aggiornamento

Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando l'aggiornamento pianificato viene avviato in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

Nota: *se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta.*

10.8.4. Pianificazione aggiornamenti Anti-Spam

Se realmente necessario, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento Anti-Spam pianificato e attivarlo nuovamente in seguito:

In questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento. Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

Questa sezione consente di specificare gli intervalli di tempo per l'avvio dell'aggiornamento Anti-Spam che è stato pianificato. È possibile specificare l'ora dall'avvio ripetuto dell'aggiornamento Anti-Spam dopo un certo periodo di tempo (***Esegui ogni***) o definendo data e ora esatte (***Esegui a un orario specifico***) oppure definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Esegui all'avvio del computer***).

Opzioni di pianificazione avanzate

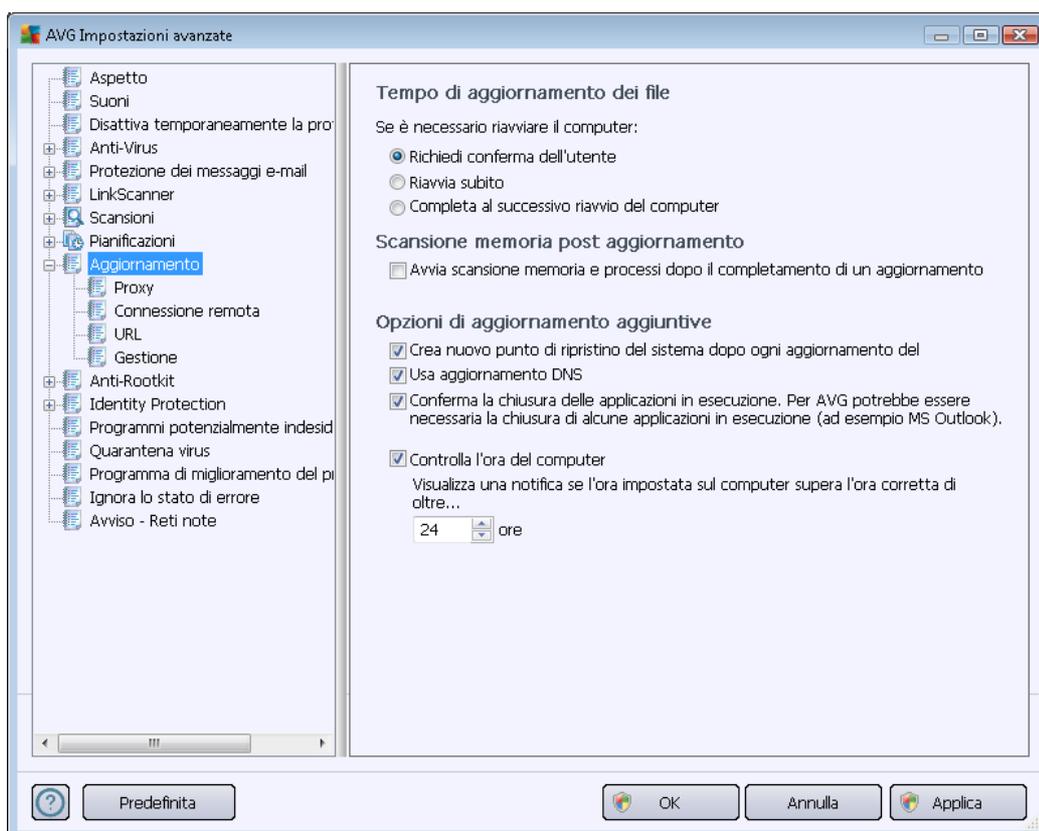
Questa sezione consente di definire le circostanze in cui deve essere avviato o non avviato l'aggiornamento Anti-Spam se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni di aggiornamento

Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento Anti-Spam non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet.

Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra a comparsa visualizzata sopra l'icona di AVG presente nella barra delle applicazioni (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

10.9. Aggiornamento

La voce ***Aggiorna*** consente di aprire una finestra di dialogo in cui è possibile specificare i parametri generali relativi all'aggiornamento di AVG:

Quando eseguire l'aggiornamento dei file

In questa sezione è possibile effettuare la selezione tra tre diverse opzioni da utilizzare nel caso in cui il processo di aggiornamento richieda il riavvio del PC. È possibile pianificare la finalizzazione

dell'aggiornamento per il successivo riavvio del PC oppure è possibile procedere subito al riavvio:

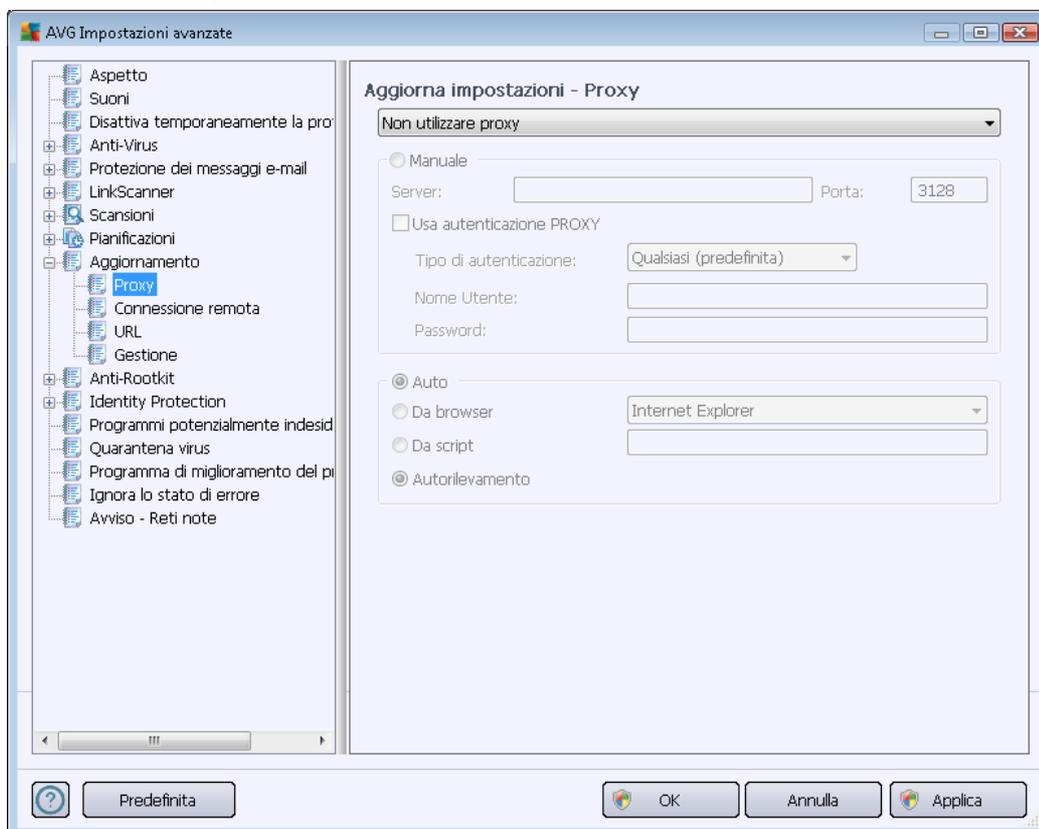
- ***Richiedi conferma dell'utente*** *(impostazione predefinita)*: verrà richiesto di approvare un riavvio del PC necessario per finalizzare il processo di aggiornamento
- ***Riavvia subito***: il computer verrà riavviato immediatamente in maniera automatica dopo la finalizzazione del processo di aggiornamento senza richiesta di conferma da parte dell'utente
- ***Completa al successivo riavvio del computer***: la finalizzazione del processo di aggiornamento verrà posticipata al successivo riavvio del computer. Tenere presente che questa opzione è consigliata solo se si è certi che il computer venga riavviato regolarmente, almeno una volta al giorno.

Scansione memoria post aggiornamento

Selezionare questa casella di controllo per specificare che si desidera avviare una nuova scansione della memoria al termine di ciascun aggiornamento. L'ultimo aggiornamento scaricato potrebbe contenere nuove definizioni dei virus e queste potrebbero applicarsi immediatamente alla scansione.

Opzioni di aggiornamento aggiuntive

- ***Crea nuovo punto di ripristino del sistema durante ogni aggiornamento del programma***: prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare il sistema operativo nella configurazione originale da questo punto. Questa opzione è accessibile tramite Start / Tutti i programmi / Accessori / Utilità di sistema / Ripristino configurazione di sistema, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti. Mantenere selezionata questa casella di controllo se si desidera utilizzare questa funzionalità.
- ***Usa aggiornamento DNS*** (*attiva per impostazione predefinita*): con questa voce selezionata, una volta avviato l'aggiornamento, **AVG Internet Security 2012** ricerca informazioni sulla versione del database dei virus più recente e sulla versione del programma più recente sul server DNS. Quindi, solo i file di aggiornamento più piccoli e indispensabili vengono scaricati e applicati. In questo modo la quantità totale di dati scaricati viene ridotta al minimo e il processo di aggiornamento viene accelerato.
- ***Conferma la chiusura delle applicazioni in esecuzione*** (*attivata per impostazione predefinita*): garantirà che nessuna applicazione in esecuzione venga chiusa senza autorizzazione, nel caso fosse necessario per la finalizzazione del processo di aggiornamento.
- ***Controlla l'ora del computer***: selezionare questa opzione per ricevere una notifica nel caso in cui l'ora del computer differisca dall'ora esatta di un valore superiore al numero di ore specificato.

10.9.1. Proxy

Il server proxy è un server autonomo o un servizio in esecuzione su un PC che garantisce una connessione più sicura a Internet. Secondo le regole di rete specificate è possibile accedere a Internet direttamente o tramite il server proxy. Sono anche consentite entrambe le possibilità contemporaneamente. Quindi, nella prima voce della finestra di dialogo ***Impostazioni aggiornamento – Proxy*** è necessario selezionare l'opzione desiderata dal menu della casella combinata:

- ***Utilizza proxy***
- ***Non utilizzare proxy***: impostazione predefinita
- ***Tenta la connessione utilizzando il proxy e, se non riesce, esegui la connessione direttamente***

Se si seleziona un'opzione utilizzando un server proxy, sarà necessario specificare ulteriori dati. Le impostazioni del server possono essere configurate manualmente o automaticamente.

Configurazione manuale

Se si seleziona la configurazione manuale (selezionare *l'opzione* ***Manuale*** *per attivare la sezione della finestra di dialogo corrispondente*) è necessario specificare le seguenti voci:

- ***Server***: specificare l'indirizzo IP o il nome del server
- ***Porta***: specifica il numero della porta che consente l'accesso a Internet (*per impostazione predefinita, il numero è impostato su 3128 ma può essere modificato – se non si è sicuri, contattare l'amministratore di rete*)

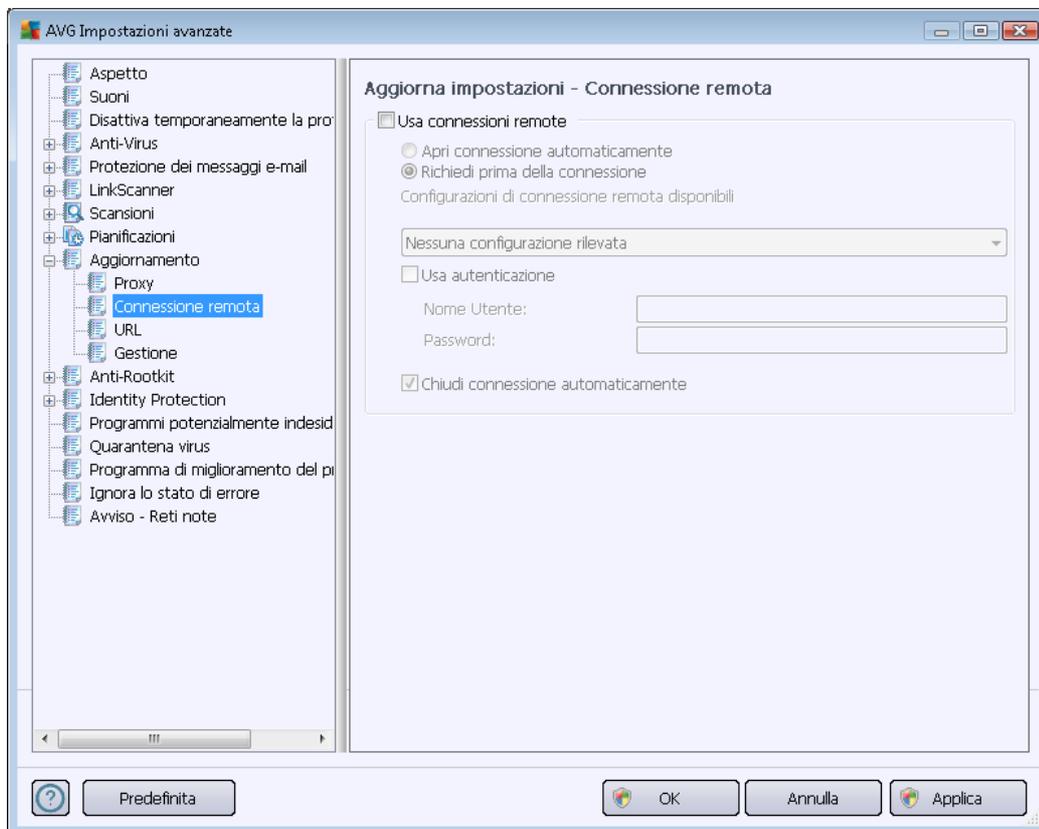
È anche possibile che sul server proxy siano state configurate regole specifiche per ciascun utente. Se il server proxy è impostato in questo modo, selezionare l'opzione ***Usa autenticazione PROXY*** per verificare che nome utente e password siano validi per la connessione a Internet tramite il server proxy.

Configurazione automatica

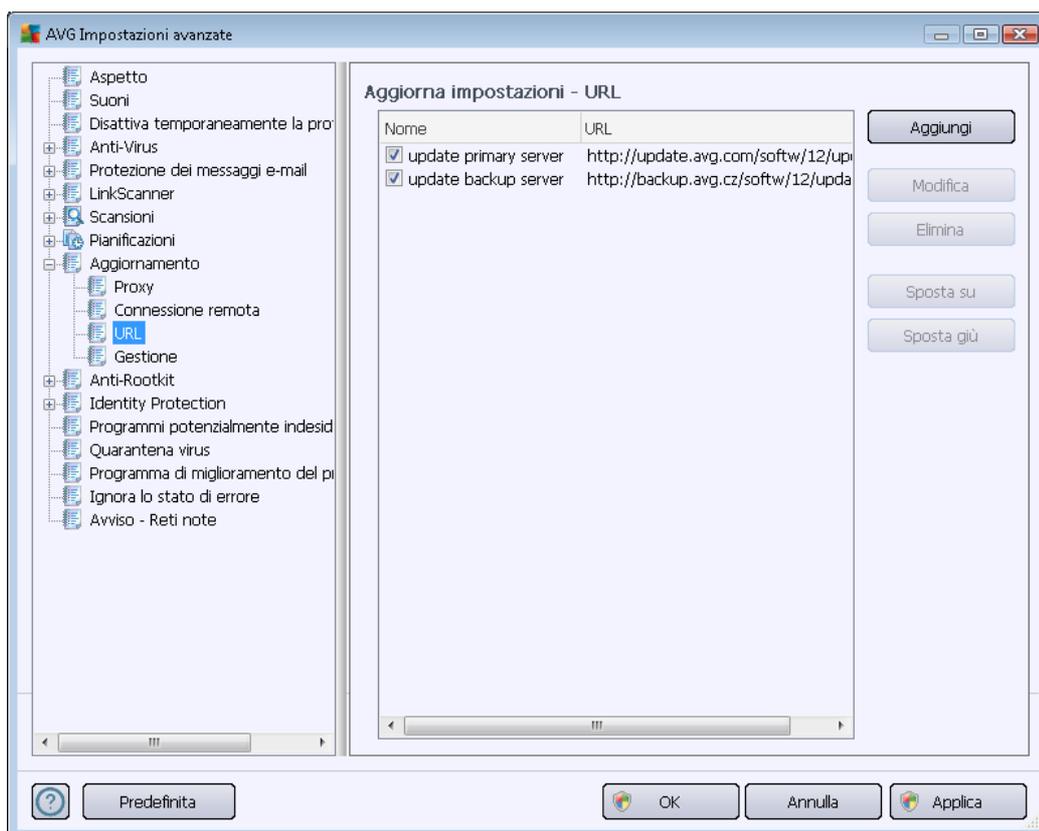
Se si seleziona la configurazione automatica *(selezionare l'opzione **Auto** per attivare la sezione della finestra di dialogo corrispondente*), selezionare quindi l'origine della configurazione proxy:

- ***Da browser***: la configurazione verrà letta dal browser Internet predefinito
- ***Da script***: la configurazione verrà letta da uno script scaricato con la funzione di restituzione dell'indirizzo proxy
- ***Autorilevamento***: la configurazione verrà rilevata automaticamente direttamente dal server proxy

10.9.2. Connessione remota

Tutti i parametri definiti facoltativamente nella finestra di dialogo ***Aggiornamento impostazioni – Connessione remota*** fanno riferimento alla connessione remota a Internet. I campi della finestra di dialogo rimangono inattivi fino a quando non viene selezionata l'opzione ***Usa connessioni remote*** che consente l'attivazione dei campi:

Specificare se si desidera connettersi automaticamente a Internet (***Apri connessione automaticamente***) o confermare la connessione manualmente ogni volta (***Richiedi prima della connessione***). Per la connessione automatica è necessario scegliere se la connessione deve essere chiusa al termine dell'aggiornamento (***Chiudi connessione automaticamente***).

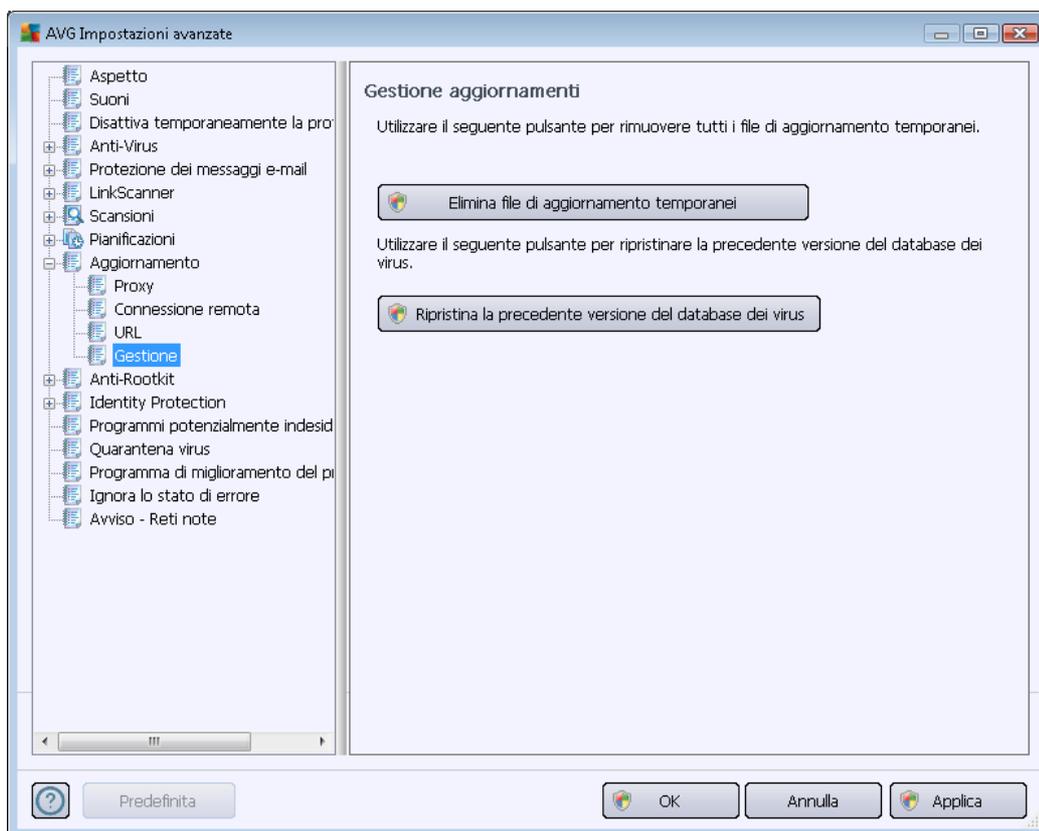
10.9.3. URL

Nella finestra di dialogo ***URL*** è contenuto un elenco di indirizzi Internet da cui è possibile scaricare i file di aggiornamento:

Pulsanti di controllo

È possibile modificare l'elenco e i suoi elementi utilizzando i seguenti pulsanti di controllo:

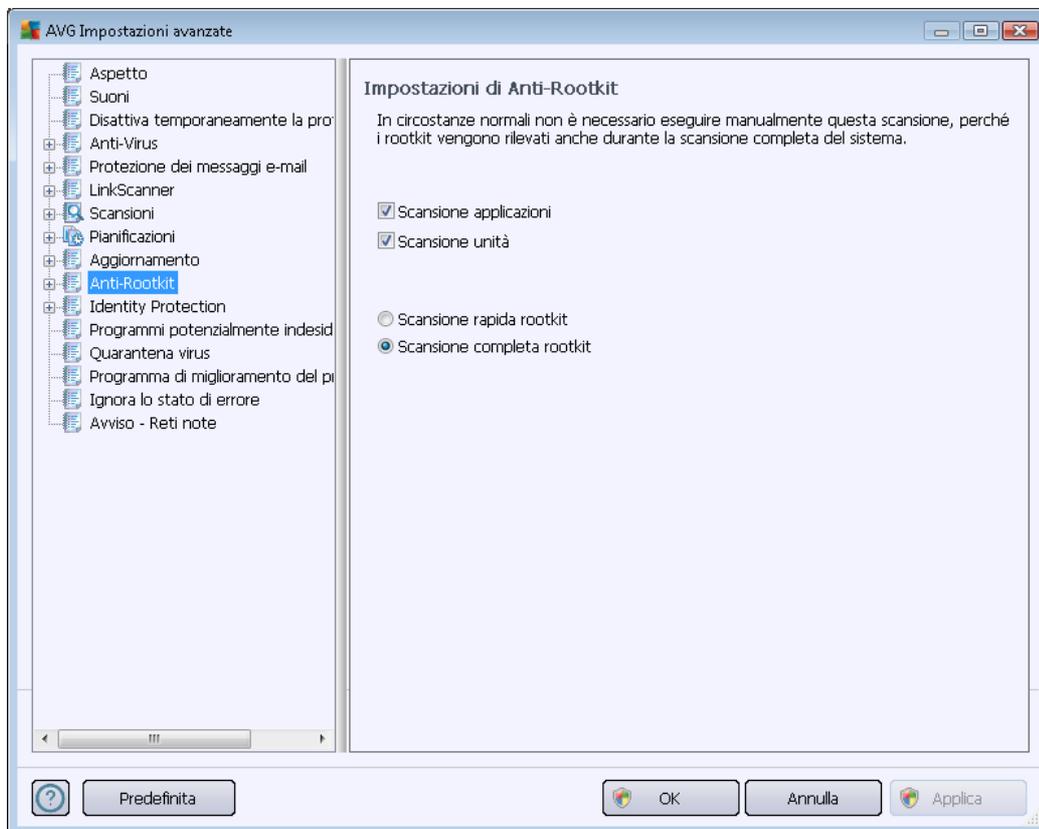
- ***Aggiungi*** :consente di aprire una finestra di dialogo in cui è possibile specificare un nuovo URL da aggiungere all'elenco
- ***Modifica***: consente di aprire una finestra di dialogo in cui è possibile modificare i parametri dell'URL selezionato
- ***Elimina***: consente di eliminare l'URL selezionato dall'elenco
- ***Sposta Su***: consente di spostare l'URL selezionato di una posizione verso l'alto nell'elenco
- ***Sposta Giù***: consente di spostare l'URL selezionato di una posizione verso il basso nell'elenco

10.9.4. Gestione

La finestra di dialogo ***Gestione aggiornamenti*** offre due opzioni accessibili tramite due pulsanti:

- ***Elimina file di aggiornamento temporanei***: selezionare questo pulsante per eliminare tutti i file di aggiornamento ridondanti dal disco rigido (*per impostazione predefinita, questi file restano memorizzati per 30 giorni*)

- ***Ripristina la precedente versione del database dei virus***: selezionare questo pulsante per eliminare l'ultima versione del database dei virus dal disco rigido e tornare alla precedente versione salvata (*la nuova versione del database dei virus verrà inserita nel successivo aggiornamento*)

10.10. Anti-Rootkit

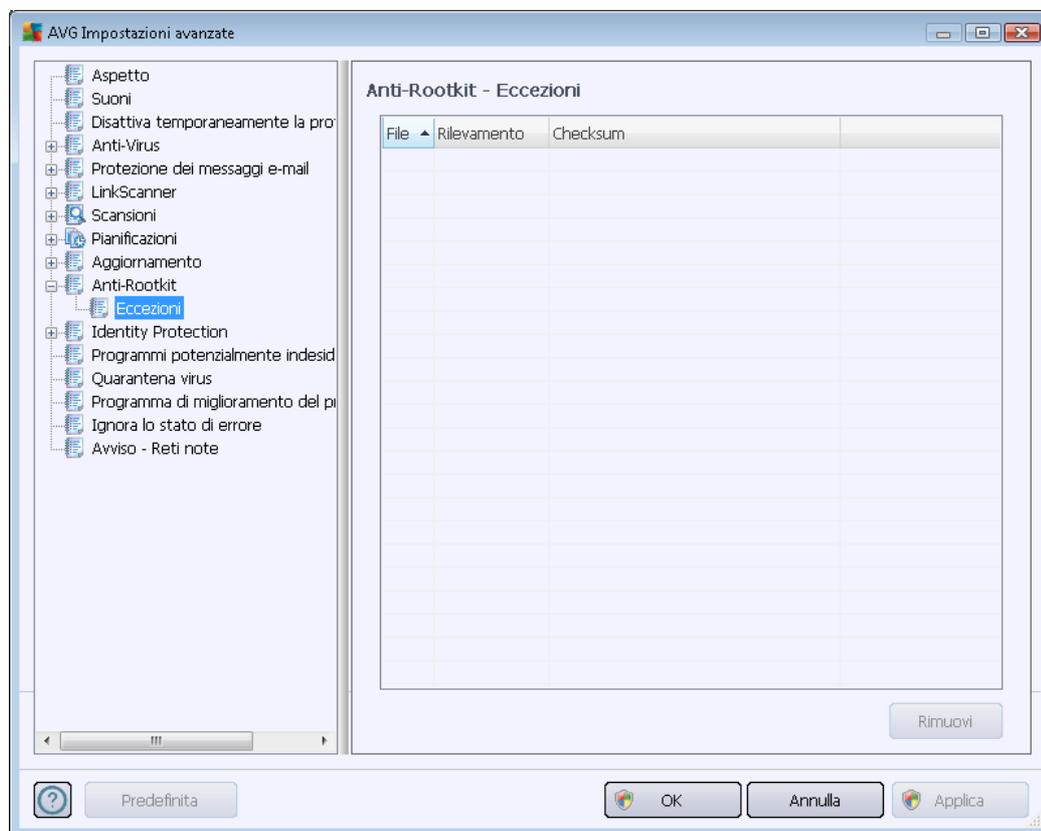
Nella finestra di dialogo ***Impostazioni di Anti-Rootkit*** è possibile modificare la configurazione del componente Anti-Rootkit e specifici parametri della scansione anti-rootkit. La scansione anti-rootkit è un processo predefinito incluso nella Scansione intero computer:

La modifica di tutte le funzioni del componente Anti-Rootkit presenti in questa finestra di dialogo è inoltre accessibile direttamente dall'interfaccia del componente Anti-Rootkit.

Scansione applicazioni e ***Scansione driver*** consentono di specificare in dettaglio gli elementi da includere nella scansione Anti-Rootkit. Queste impostazioni sono progettate per utenti esperti. Si consiglia di lasciare attivate tutte le opzioni. Quindi, è possibile selezionare la modalità di scansione anti-rootkit:

- ***Scansione rapida rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*)

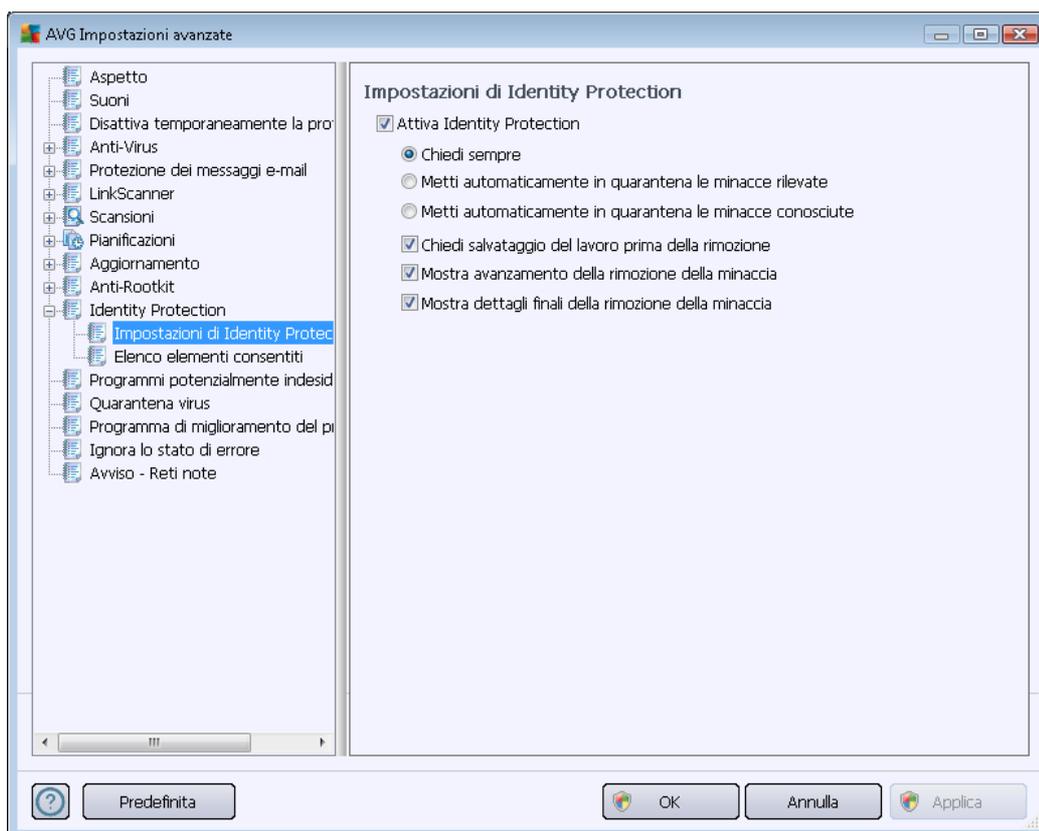
- ***Scansione completa rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*), nonché tutte le unità locali (*inclusa l'unità di memoria flash, ma escluse le unità disco floppy/CD*)

10.10.1. Eccezioni

Nella finestra di dialogo ***Anti-Rootkit – Eccezioni*** è possibile indicare file specifici *(ad esempio alcuni driver che potrebbero essere rilevati erroneamente come rootkit)* da escludere dalla scansione:

10.11. Identity Protection

Identity Protection è un componente anti-malware che protegge il computer da qualsiasi tipo di malware (*spyware, bot, furti di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus *(per una descrizione dettagliata delle funzionalità del componente, vedere il capitolo Identity Protection*).

10.11.1. Impostazioni di Identity Protection

La finestra di dialogo ***Impostazioni di Identity Protection*** consente di attivare/disattivare le funzioni di base del componente Identity Protection:

Attiva Identity Protection (*attivata per impostazione predefinita*): deselezionare la casella per disattivare il componente Identity Protection.

Si consiglia di non disattivare questo componente a meno che non sia assolutamente necessario.

Quando Identity Protection è attivato, è possibile specificare l'azione da intraprendere quando viene rilevata una minaccia:

- ***Chiedi sempre***: (*attivata per impostazione predefinita*) quando viene rilevata una minaccia, verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione da eseguire venga rimossa.

- ***Metti automaticamente in quarantena le minacce rilevate***: selezionare questa casella di controllo per spostare immediatamente tutte le potenziali minacce rilevate nell'area sicura di Quarantena virus di. Se si mantengono le impostazioni predefinite, quando una minaccia viene rilevata verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione da eseguire venga rimossa.

- ***Metti automaticamente in quarantena le minacce conosciute***: mantenere selezionata

questa voce se si desidera che tutte le applicazioni rilevate come possibili malware vengano messe subito in Quarantena virus di automaticamente.

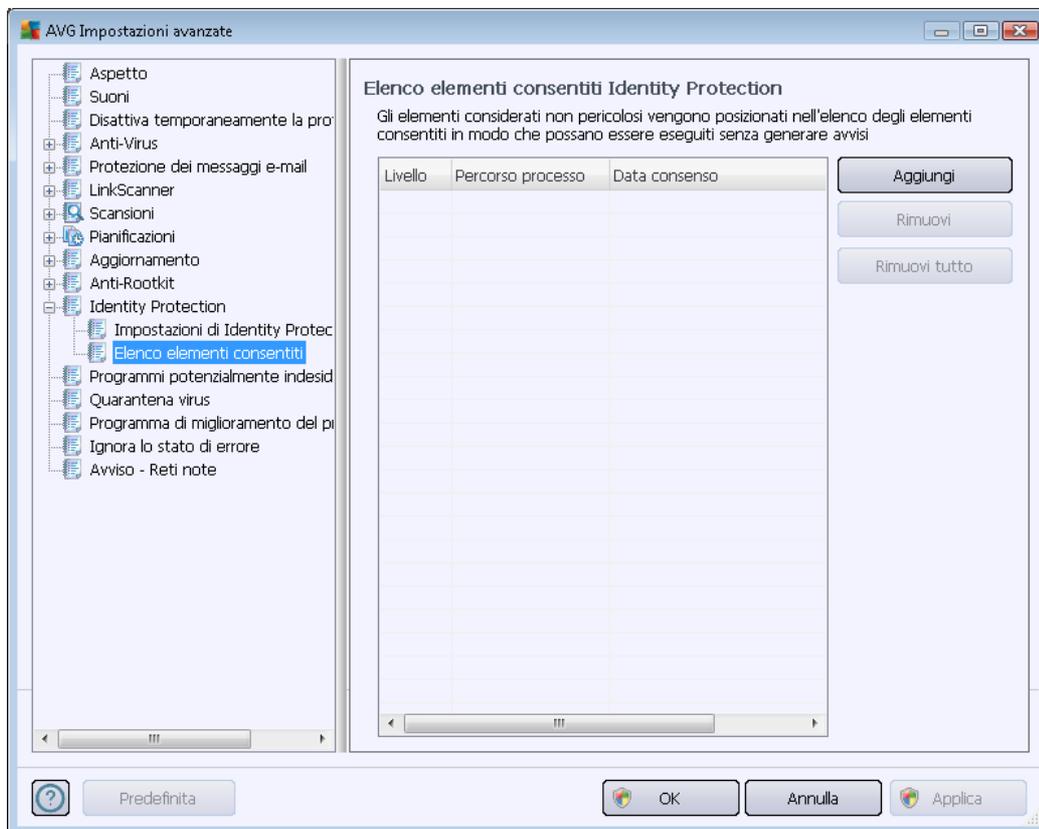
È inoltre possibile utilizzare voci specifiche per attivare facoltativamente ulteriori funzionalità di Identity Protection:

- ***Chiedi salvataggio del lavoro prima della rimozione*** (*attivata per impostazione predefinita*): mantenere selezionata questa voce se si desidera essere avvertiti prima che l'applicazione rilevata come possibile malware venga messa in quarantena. Se l'applicazione è in uso, il progetto potrebbe venire perso, pertanto è necessario salvarlo. Questa voce è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione.

- ***Mostra avanzamento della rimozione della minaccia*** (*attivata per impostazione predefinita*): se questa opzione è attivata, quando viene rilevato un potenziale malware si apre una nuova finestra di dialogo per visualizzare l'avanzamento dello spostamento del malware in quarantena.

- ***Mostra i dettagli finali della rimozione della minaccia*** : (*attivata per impostazione predefinita*) se questa opzione è attivata, ***Identity Protection*** visualizza informazioni dettagliate su ciascun oggetto spostato in quarantena (*livello di gravità, posizione e così via*).

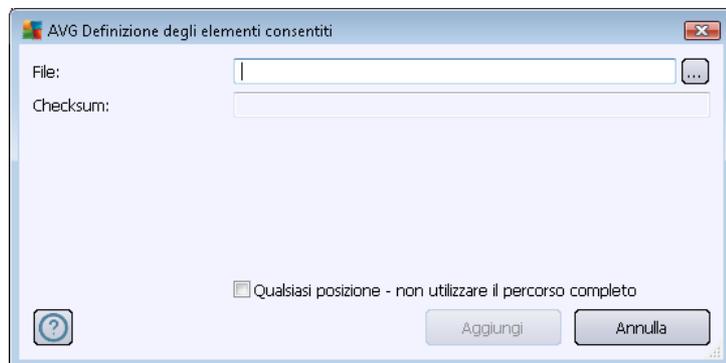
10.11.2. Elenco elementi consentiti

Se nella finestra di dialogo delle ***impostazioni di Identity Protection*** non è stata selezionata la voce ***Metti automaticamente in quarantena le minacce rilevate***, ogni qualvolta verrà rilevato un malware potenzialmente pericoloso verrà richiesto se tale malware dovrà essere rimosso. Se si contrassegna l'applicazione sospetta (*rilevata in base al comportamento*) come sicura e si conferma che è possibile mantenerla nel computer, l'applicazione verrà aggiunta all'***elenco degli elementi consentiti di Identity Protection*** e non verrà più segnalata come potenzialmente pericolosa:

L'***elenco degli elementi consentiti di Identity Protection*** fornisce le seguenti informazioni su ciascuna applicazione:

- ***Livello***: identificazione grafica della gravità di un determinato processo valutata su una scala di quattro livelli dal meno grave (■□□□) al più grave (■■■■)
- ***Percorso processo***: posizione del file eseguibile (*processo*) dell'applicazione
- ***Data consenso***: data in cui l'applicazione è stata contrassegnata manualmente come sicura

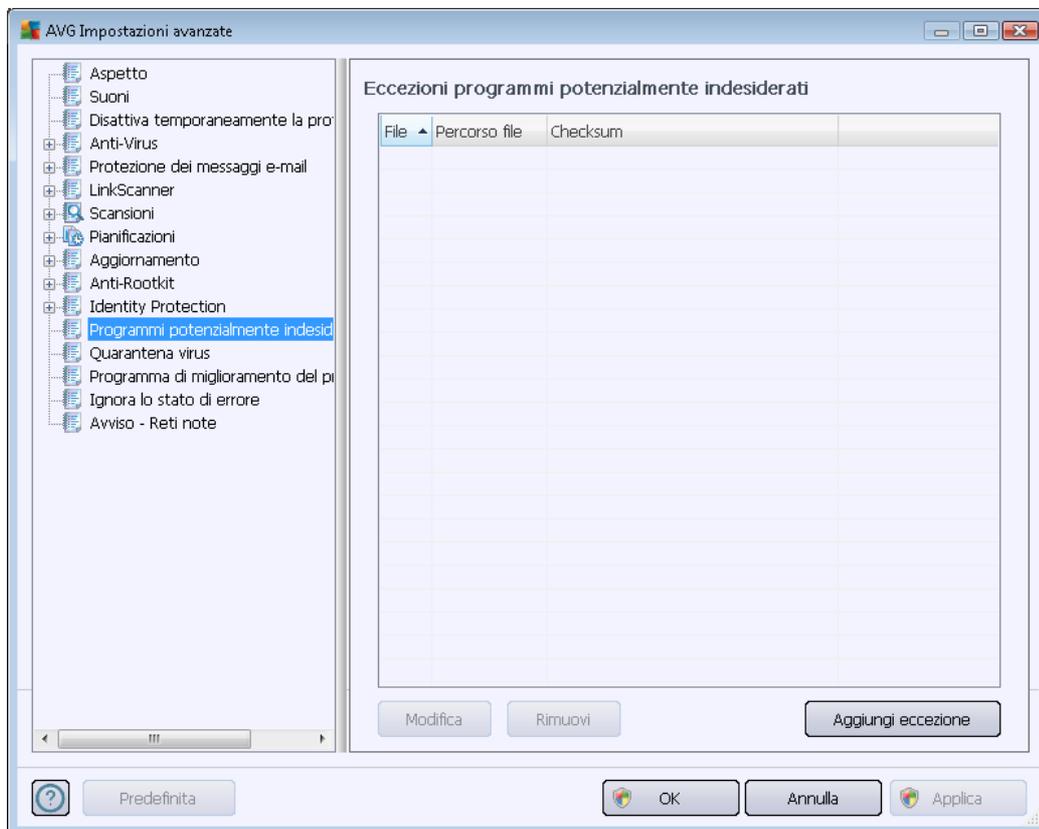
Pulsanti di controllo

I pulsanti di controllo disponibili nella finestra di dialogo dell'***elenco degli elementi consentiti di Identity Protection*** sono i seguenti:

- ***Aggiungi***: fare clic su questo pulsante per aggiungere una nuova applicazione all'elenco degli elementi consentiti. Viene visualizzata la seguente finestra di dialogo:

- *File*: digitare il percorso completo del file (*applicazione*) da contrassegnare come eccezione.
- ***Checksum***: visualizza la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente a AVG di distinguere in modo inequivocabile il file scelto dagli altri file. Il checksum viene generato e visualizzato dopo che il file è stato aggiunto.
- ***Qualsiasi posizione – non utilizzare il percorso completo***: per definire il file come eccezione solo per la posizione specifica, lasciare deselezionata questa casella di controllo.

- ***Rimuovi***: selezionare questa opzione per rimuovere l'applicazione selezionata dall'elenco.
- ***Rimuovi tutto***: selezionare questa opzione per rimuovere tutte le applicazioni elencate.

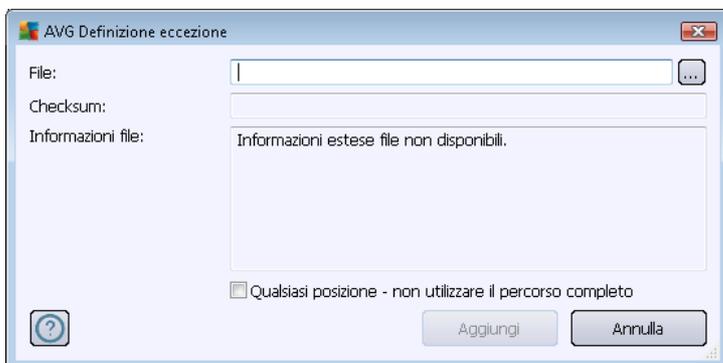
10.12. Programmi potenzialmente indesiderati

AVG Internet Security 2012 è in grado di analizzare e rilevare le applicazioni eseguibili o le librerie DLL che potrebbero essere potenzialmente indesiderate nel sistema. In alcuni casi l'utente può scegliere di mantenere alcuni programmi indesiderati sul computer (programmi che sono stati installati intenzionalmente). Alcuni programmi, soprattutto quelli gratuiti, includono adware. Tale adware può essere rilevato e segnalato da **AVG Internet Security 2012** come *programma potenzialmente indesiderato*. Se si desidera mantenere tali programmi sul computer, è possibile definirli come eccezioni ai programmi potenzialmente indesiderati:

Nella finestra di dialogo ***Eccezioni ai programmi potenzialmente indesiderati*** viene visualizzato un elenco di eccezioni già definite e attualmente valide ai programmi potenzialmente indesiderati. È possibile modificare l'elenco, eliminare voci esistenti o aggiungere nuove eccezioni. L'elenco fornisce le seguenti informazioni per ciascuna eccezione:

- ***File***: fornisce il nome preciso della rispettiva applicazione
- ***Percorso file***: mostra la posizione dell'applicazione
- ***Checksum***: visualizza la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente a AVG di distinguere in modo inequivocabile il file prescelto dagli altri file. Il checksum viene generato e visualizzato dopo che il file è stato aggiunto.

Pulsanti di controllo

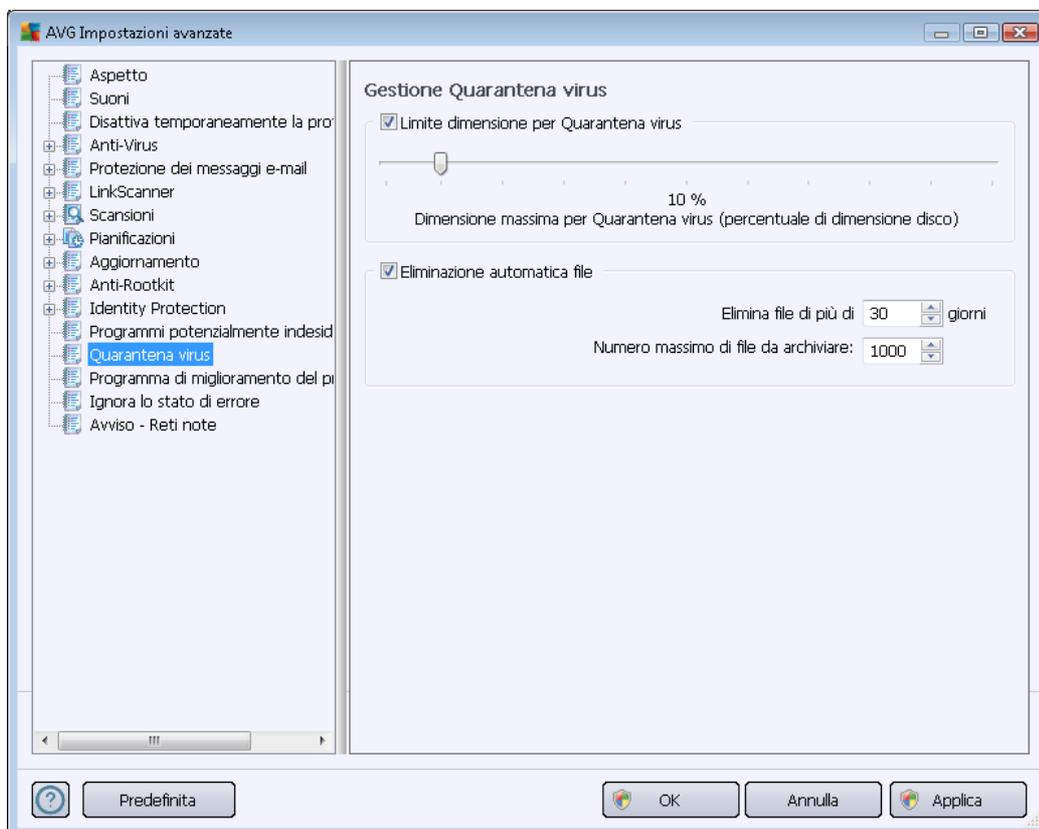
- ***Modifica***: consente di aprire una finestra di dialogo per la modifica (*identica alla finestra di dialogo per la definizione di una nuova eccezione, vedere di seguito*) di un'eccezione già definita. In tale finestra è possibile modificare i parametri dell'eccezione
- ***Rimuovi***: consente di eliminare la voce selezionata dall'elenco di eccezioni.
- ***Aggiungi eccezione***: consente di aprire una finestra di dialogo per la modifica in cui è

possibile definire i parametri della nuova eccezione da creare:

- *File*: digitare il percorso completo del file da contrassegnare come eccezione.

- *Checksum*: visualizza la "firma" univoca del file prescelto. Questo checksum è una stringa di caratteri generata automaticamente che consente a AVG di distinguere in modo inequivocabile il file prescelto dagli altri file. Il checksum viene generato e visualizzato dopo che il file è stato aggiunto.

- *Informazioni file*: vengono visualizzate eventuali informazioni aggiuntive disponibili sul file *(licenza, versione e così via)*

- *Qualsiasi posizione – non utilizzare il percorso completo*: per definire il file come eccezione solo per la posizione specifica, lasciare deselezionata questa casella di controllo. Se la casella di controllo è selezionata, il file specificato viene definito come eccezione indipendentemente dalla relativa posizione *(tuttavia, è comunque necessario immettere il percorso completo dello specifico file; il file verrà quindi utilizzato come esemplare univoco nel caso in cui due file con lo stesso nome compaiano nel sistema)*.

10.13. Quarantena virus

La finestra di dialogo ***Gestione Quarantena virus*** consente di definire diversi parametri relativi alla gestione degli oggetti archiviati in Quarantena virus:

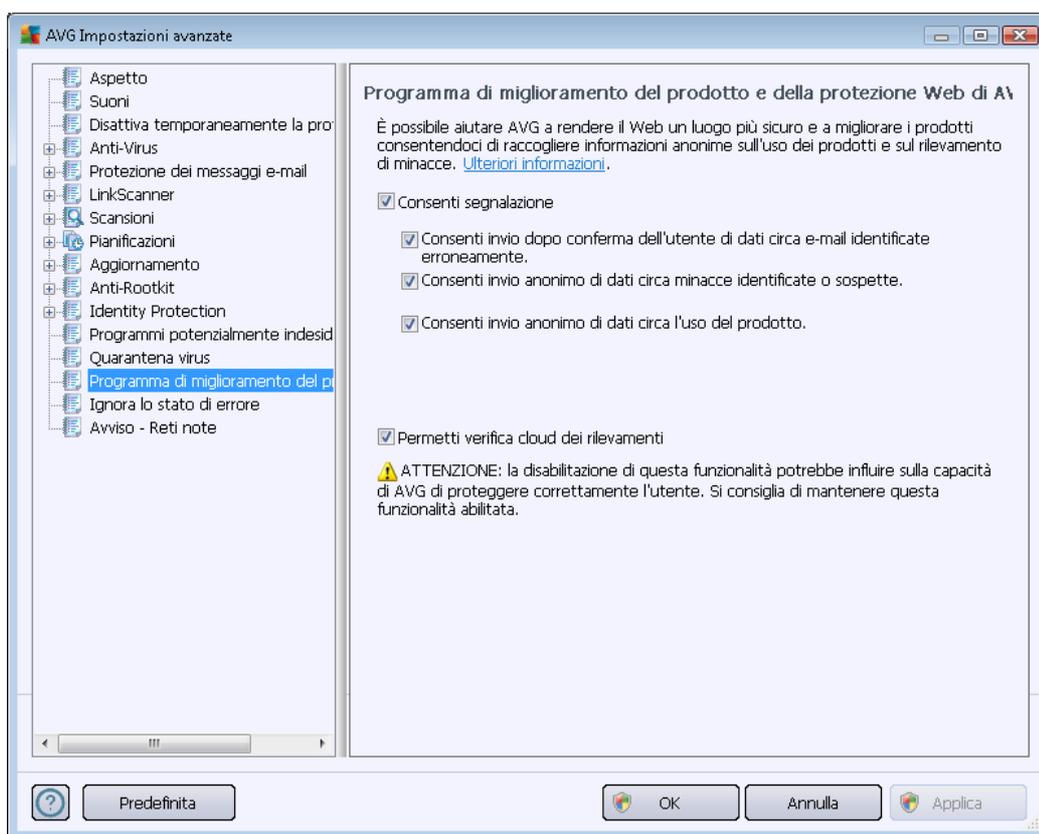
- ***Limite dimensione per Quarantena virus***: utilizzare il dispositivo di scorrimento per impostare la dimensione massima di Quarantena virus. La dimensione è specificata in maniera proporzionale rispetto alla dimensione del disco locale.

- ***Eliminazione automatica file***: questa sezione consente di definire la durata massima di memorizzazione degli oggetti in Quarantena virus (***Elimina file di più di... giorni***) e il numero massimo di file da memorizzare in Quarantena virus (***Numero massimo di file da memorizzare***).

10.14. Programma di miglioramento del prodotto

La finestra di dialogo ***Programma di miglioramento del prodotto e della protezione Web di AVG*** invita a collaborare al miglioramento del prodotto AVG per aiutarci ad aumentare il livello di protezione generale in Internet. Mantenere l'opzione ***Consenti segnalazione*** selezionata per consentire la segnalazione delle minacce rilevate ai laboratori AVG. Questo ci consente di raccogliere informazioni aggiornate sulle minacce più recenti da tutti gli utenti a livello mondiale e di migliorare la protezione per tutti.

La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo

all'utente. Inoltre, nei rapporti non vengono inclusi dati personali. La segnalazione delle minacce rilevate è opzionale. Tuttavia si consiglia si mantenere attivata questa opzione. La segnalazione ci aiuta a migliorare la protezione per tutti gli utenti AVG.

Nella finestra di dialogo sono disponibili le seguenti opzioni di impostazione:

- ***Consenti segnalazione*** *(attiva per impostazione predefinita)* : se si desidera collaborare al miglioramento del prodotto **AVG Internet Security 2012**, mantenere selezionata questa casella di controllo. Ciò consentirà di segnalare ad AVG tutte le minacce riscontrate. In questo modo saremo in grado di raccogliere informazioni aggiornate sui malware da tutti gli utenti a livello mondiale e di migliorare la protezione di conseguenza. La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente e nei rapporti non vengono inclusi dati personali.
    - ***Consenti invio dopo conferma dell'utente di dati circa e-mail identificate erroneamente*** *(attiva per impostazione predefinita)*: invia informazioni sui messaggi e-mail identificati erroneamente come spam o sui messaggi di spam non rilevati dal componente Anti-Spam. Per l'invio di questo tipo di informazioni verrà richiesta la conferma dell'utente.
    - ***Consenti invio anonimo di dati circa minacce identificate o sospette*** *(attiva per impostazione predefinita)*: invia informazioni su comportamenti o codici certamente pericolosi o sospetti *(può trattarsi di un virus, uno spyware o una pagina Web dannosa a cui si sta tentando di accedere) rilevati nel computer.*

- *Consenti invio anonimo di dati circa l'uso del prodotto* (attiva per impostazione predefinita) : invia statistiche di base sull'uso dell'applicazione, ad esempio numero di rilevamenti, scansioni avviate, aggiornamenti riusciti/non riusciti e così via.

- ***Permetti verifica cloud dei rilevamenti*** *(attiva per impostazione predefinita)*: le minacce rilevate verranno controllate per verificare l'effettiva presenza di infezioni, in modo da evitare i falsi positivi.

Minacce Web più diffuse

Attualmente le minacce esistenti non si limitano più ai semplici virus. Gli autori di codici dannosi e di siti Web pericolosi hanno molta inventiva, per cui emergono abbastanza di frequente nuovi tipi di minacce, la maggior parte delle quali in Internet. Di seguito vengono riportati alcuni dei tipi più comuni:

- ***Un virus*** è un codice dannoso che si copia e si diffonde in maniera automatica, spesso passando inosservato fino al compimento del danno. Alcuni virus rappresentano una minaccia seria, poiché eliminano o modificano direttamente i file, mentre altri agiscono in maniera apparentemente innocua, ad esempio durante la riproduzione di un brano musicale. Tuttavia, tutti i virus sono pericolosi a causa della capacità di base di moltiplicarsi. Anche un virus semplice è in grado di assorbire tutta la memoria di un computer in un istante causando danni.

- ***Il worm*** è una sottocategoria di virus che, a differenza dei virus normali, non necessita di un oggetto "trasportatore" a cui collegarsi; si invia automaticamente ad altri computer, solitamente tramite e-mail, provocando spesso sovraccarichi sui server e-mail e sui sistemi di rete.

- ***Spyware*** si definisce solitamente come una categoria di malware (*malware = qualsiasi software dannoso, virus compresi*) che comprende alcuni programmi, in genere trojan horse, il cui scopo è quello di appropriarsi di informazioni personali, password, numeri delle carte di credito o infiltrarsi in un computer consentendo all'autore dell'attacco di assumere il controllo in modalità remota, ovviamente senza che il proprietario del computer ne sia a conoscenza o abbia dato il proprio consenso.

- ***I programmi potenzialmente indesiderati*** sono un tipo di spyware che può essere o meno pericoloso per il computer. Un esempio specifico di PUP è l'adware, un software progettato per distribuire annunci, solitamente tramite la visualizzazione di popup. Può essere fastidioso ma non realmente dannoso.

- ***I cookie di rilevamento*** possono inoltre essere considerati come un tipo di spyware, in quanto si tratta di piccoli file archiviati nel browser Web e inviati automaticamente al sito Web principale quando lo si visita di nuovo, e possono contenere dati quali la cronologia di esplorazione e altre informazioni simili.

- ***Exploit*** è un codice dannoso che sfrutta un'imperfezione o una vulnerabilità di un sistema operativo, un browser Internet o un altro programma fondamentale.

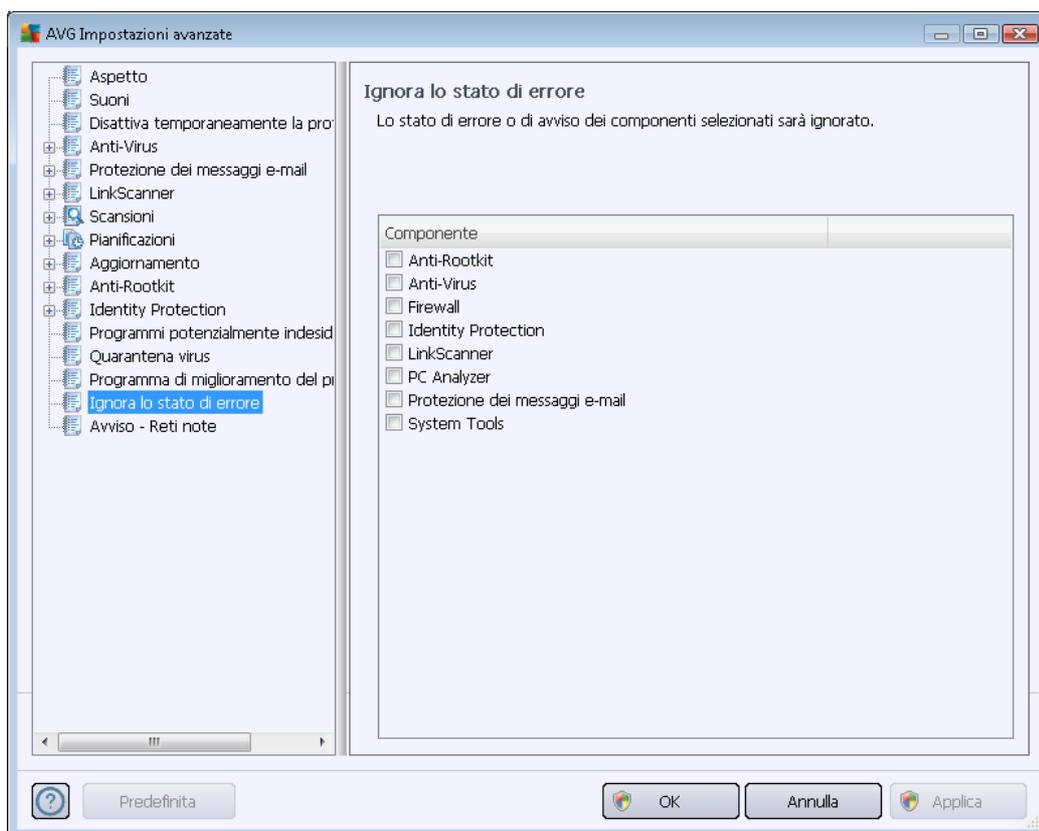
- ***Il phishing*** è un tentativo di acquisire dati personali sensibili fingendosi un'organizzazione nota e affidabile. In genere, le vittime potenziali vengono contattate tramite messaggi e-mail

inviati in blocco in cui vengono richiesti, ad esempio, i dati del conto bancario. A questo scopo, gli utenti vengono invitati a seguire il collegamento fornito che li indirizza a un sito Web della banca falso.

- ***Gli hoax*** sono messaggi e-mail inviati in blocco contenenti informazioni pericolose, allarmanti o semplicemente inutili e fastidiose. Molte delle minacce sopraelencate per diffondersi utilizzano i messaggi e-mail hoax.
- ***I siti Web dannosi*** sono quei siti che installano deliberatamente software dannoso nel computer, in modo simile ai siti manomessi, anche se questi ultimi sono siti Web legittimi che sono stati compromessi da visitatori che hanno introdotto infezioni.

Per proteggere il PC da tutti questi tipi di minaccia, AVG Internet Security 2012 include componenti dedicati. Per una breve descrizione, consultare il capitolo Panoramica dei componenti.

10.15. Ignora lo stato di errore

Nella finestra di dialogo ***Ignora lo stato di errore*** è possibile selezionare i componenti in merito ai quali non si desidera ricevere informazioni:

Per impostazione predefinita, in questo elenco non è selezionato alcun componente. Ciò significa che se per un qualsiasi componente si verifica uno stato di errore, se ne verrà immediatamente informati tramite:

- l'icona presente nella barra delle applicazioni: quando tutte le parti di AVG funzionano correttamente, l'icona viene visualizzata in quattro colori; se si verifica un errore, l'icona viene visualizzata con un punto esclamativo giallo,
- una descrizione del problema esistente visualizzata nella sezione Informazioni sullo stato di protezione della finestra principale di AVG

Potrebbe verificarsi una situazione in cui, per qualsiasi motivo, risulti necessario disattivare un componente temporaneamente (*questa operazione tuttavia non è consigliata: si dovrebbe tentare di mantenere tutti i componenti attivati in modo permanente e con la configurazione predefinita*). In tal caso, l'icona presente nella barra delle applicazioni segnala automaticamente lo stato di errore del componente. In casi del genere, tuttavia, non è possibile parlare di errore effettivo, poiché la condizione è stata indotta deliberatamente dall'utente e si è consapevoli del potenziale rischio. Nel contempo, una volta che viene visualizzata in grigio, l'icona non può più segnalare eventuali errori ulteriori che potrebbero verificarsi.

Per gestire situazioni simili, all'interno della suddetta finestra di dialogo è possibile selezionare i componenti che potrebbero trovarsi in stato di errore (*o disattivati*) in merito ai quali non si desidera ricevere informazioni. Per *ignorare lo stato di componenti specifici* è inoltre possibile utilizzare direttamente la panoramica dei componenti presente nella finestra principale di AVG.

10.16. Avviso – Reti note

In AVG Advisor è inclusa una funzionalità che monitora le reti a cui si esegue la connessione e, se viene rilevata una nuova rete *(con un nome di rete già utilizzato, che potrebbe generare confusione)*, visualizza una notifica e suggerisce di verificare la sicurezza della rete. Se si considera sicura la nuova rete, è possibile salvarla in questo elenco. AVG Advisor ne memorizzerà gli attributi univoci *(in particolare l'indirizzo MAC)* e la notifica non verrà più visualizzata.

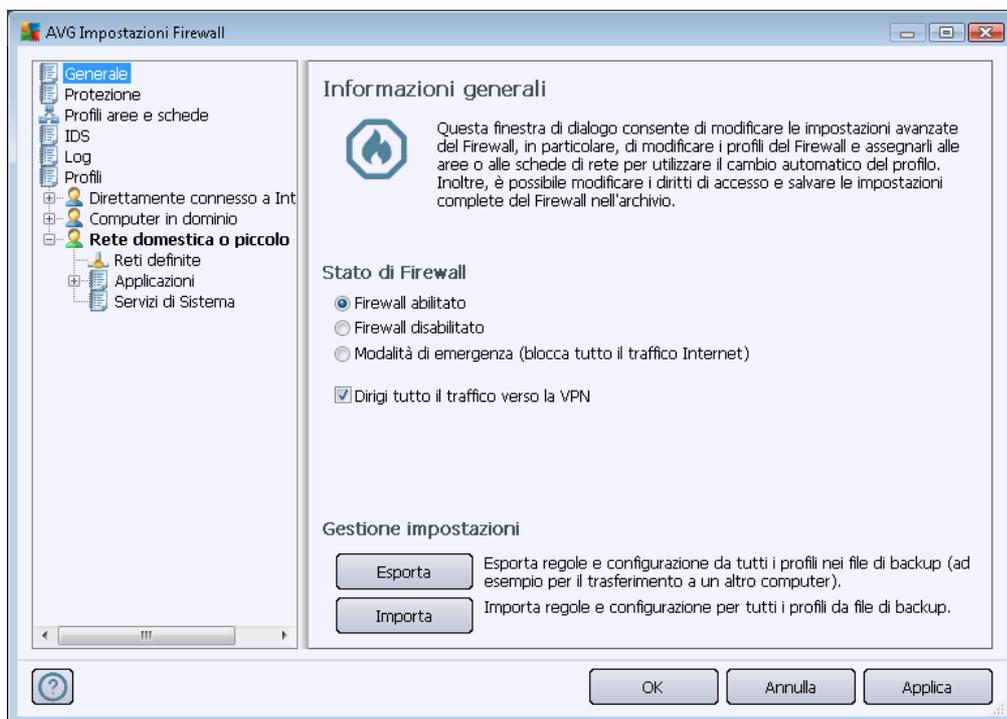
In questa finestra di dialogo è possibile controllare le reti precedentemente salvate come note. È possibile eliminare singole voci facendo clic sul pulsante ***Rimuovi***: la rete corrispondente verrà nuovamente considerata sconosciuta e potenzialmente non sicura.

11. Impostazioni Firewall

La finestra di dialogo di configurazione di Firewall viene aperta in una nuova finestra dove in varie finestre di dialogo è possibile impostare parametri del componente molto avanzati.

Tuttavia, il produttore del software ha impostato tutti i componenti di AVG Internet Security 2012 per fornire prestazioni ottimali. A meno che non sussista un motivo valido, si consiglia di non modificare la configurazione predefinita. Le eventuali modifiche alle impostazioni devono essere eseguite solo da utenti esperti.

11.1. Generale

La finestra di dialogo ***Informazioni generali*** è divisa in due sezioni:

Stato del firewall:

Nella sezione ***Stato del firewall*** è possibile modificare lo stato del Firewall in base alle esigenze:

- ***Firewall abilitato***: selezionare questa opzione per consentire la comunicazione alle applicazioni contrassegnate come "consentite" nell'insieme di regole definito all'interno del profilo Firewall selezionato.
- ***Firewall disabilitato***: questa opzione consente di disattivare completamente il componente Firewall. Tutto il traffico di rete viene consentito ma non controllato.
- ***Modalità di emergenza (blocca tutto il traffico Internet)***: selezionare questa opzione per

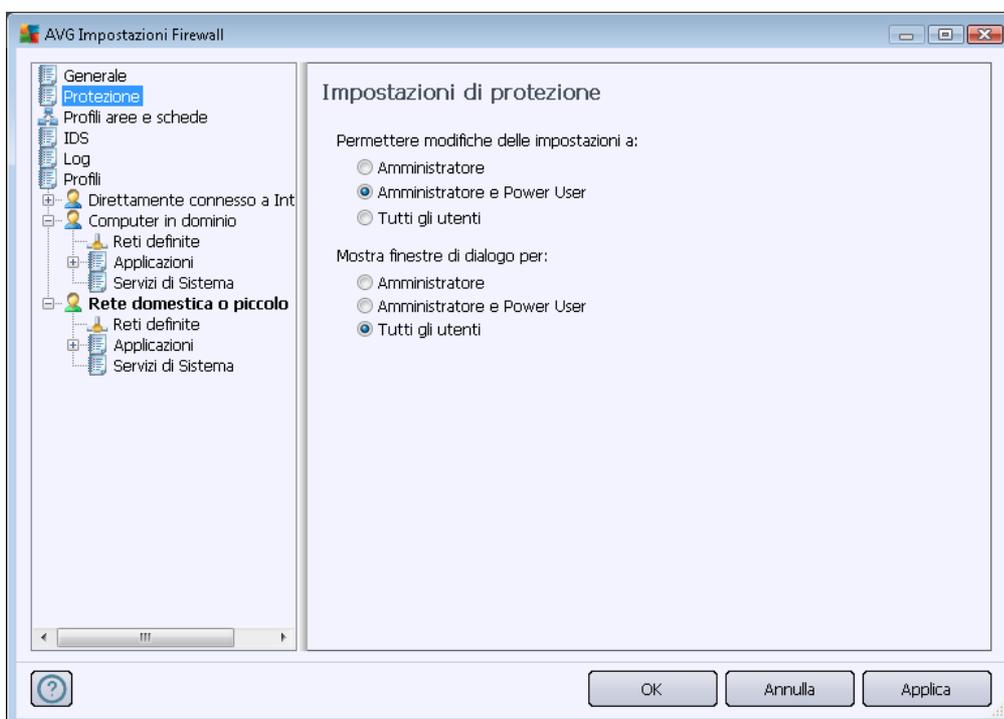
bloccare tutto il traffico su ogni singola porta di rete; il Firewall è ancora in esecuzione ma tutto il traffico di rete viene interrotto.

- ***Dirigi tutto il traffico verso la VPN*** *(attivata per impostazione predefinita)*: se si utilizza una connessione VPN *(Virtual Private Network)*, ad esempio per connettersi all'ufficio da casa, si consiglia di selezionare questa casella. ***AVG Firewall*** cercherà automaticamente tra le schede di rete, troverà quelle utilizzate per la connessione VPN e consentirà a tutte le applicazioni di connettersi alla rete di destinazione *(valido solo per le applicazioni senza specifiche regole Firewall assegnate)*. Su un sistema standard con schede di rete comuni, questo semplice passaggio dovrebbe evitare di dover impostare una regola dettagliata per ciascuna applicazione da utilizzare sulla VPN.

Nota: *per attivare la connessione VPN completamente, è necessario consentire la comunicazione ai seguenti protocolli di sistema: GRE, ESP, L2TP, PPTP. Questa operazione può essere effettuata nella finestra di dialogo Servizi di sistema.*

Gestione impostazioni

Nella sezione ***Informazioni generali*** è possibile utilizzare le opzioni ***Esporta*** o ***Importa*** per la configurazione del componente Firewall, ossia esportare le regole e le impostazioni Firewall definite nei file di backup oppure, dall'altra parte, importare il file dell'intero backup.

11.2. Protezione

Nella finestra di dialogo ***Impostazioni di protezione*** è possibile definire regole generali del comportamento di Firewall, indipendentemente dal profilo selezionato:

- ***Permettere modifiche delle impostazioni a***: consente di specificare a chi è consentito modificare la configurazione del Firewall.

- ***Mostra finestre di dialogo per***: consente di specificare gli utenti per i quali devono essere visualizzate le finestre di dialogo di conferma (*finestre di dialogo in cui si chiede una decisione in una situazione che non è coperta da una regola definita del Firewall*).

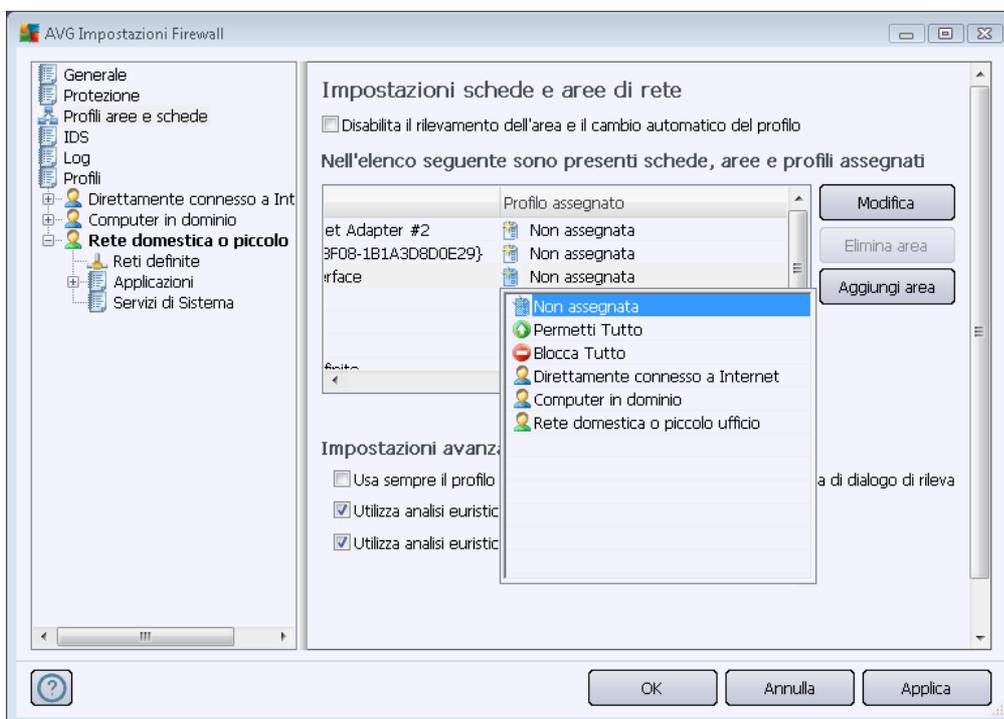
In entrambi i casi è possibile assegnare il diritto specifico a uno dei seguenti gruppi di utenti:

- ***Amministratore***: consente di controllare completamente il PC e dispone dei diritti per assegnare ogni utente ai vari gruppi con autorità definite in modo specifico.

- ***Amministratore e Power User***: l'amministratore può assegnare qualunque utente a un gruppo specifico (*Power User*) e definire le autorità dei membri del gruppo.

- ***Tutti gli utenti***: altri utenti non assegnati a un gruppo specifico.

11.3. Profili di aree e schede

Nella finestra di dialogo ***Impostazioni delle aree di rete e delle schede*** è possibile modificare impostazioni correlate all'assegnazione di profili definiti a schede specifiche con riferimento alle rispettive reti:

- ***Disabilita il rilevamento dell'area e il cambio automatico del profilo*** (*disattivata per impostazione predefinita)*: uno dei profili definiti può essere assegnato a ciascun tipo di

interfaccia di rete, rispettivamente a ciascuna area. Se non si desidera definire profili specifici, verrà utilizzato un profilo comune. Tuttavia, se si decide di distinguere i profili e assegnarli a schede e aree specifiche e in seguito, per qualsiasi motivo, si desidera cambiare temporaneamente questa impostazione, selezionare l'opzione ***Disabilita rilevamento delle aree e attivazione dei profili***.

- ***Elenco di schede, aree e profili assegnati***: in questo elenco è disponibile una panoramica delle schede e delle aree rilevate. A ciascuna di esse è possibile assegnare un profilo specifico dal menu dei profili definiti. Per aprire il menu, fare clic sulla voce pertinente nell'elenco delle schede *(nella colonna Profilo assegnato)*, quindi selezionare il profilo dal menu di scelta rapida.

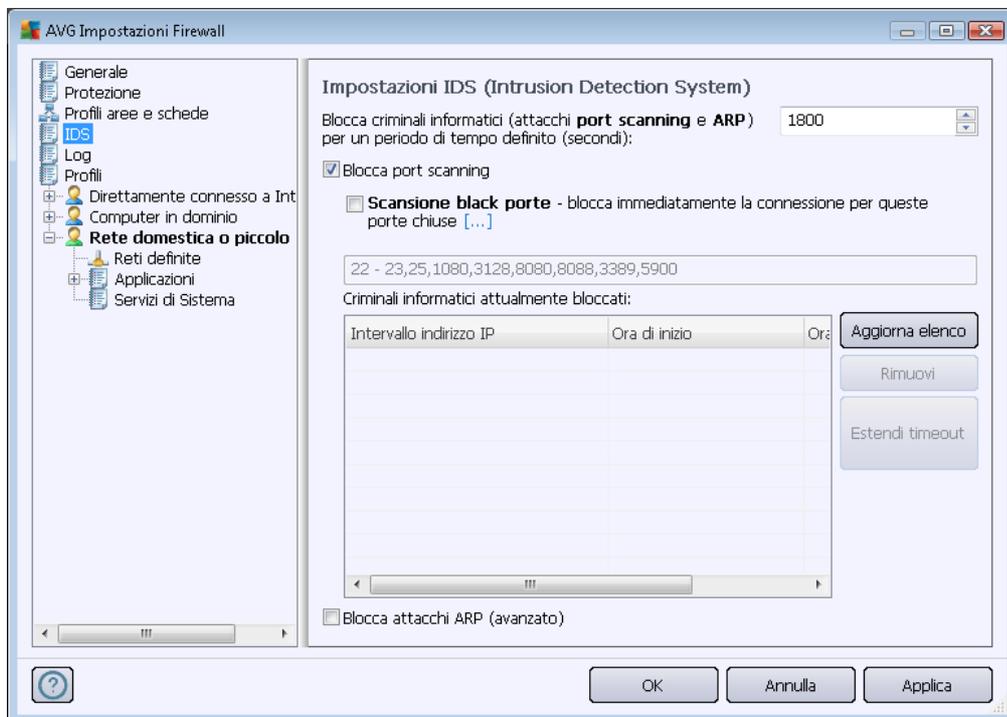
Impostazioni avanzate

- ***Usa sempre il profilo predefinito e non visualizzare la nuova finestra di dialogo di rilevamento rete***: ogni volta che il computer stabilisce una connessione a una nuova rete, il Firewall visualizza una finestra di dialogo in cui viene richiesto di selezionare un tipo di connessione di rete e di assegnare alla connessione un profilo Firewall. Se non si desidera che tale finestra venga visualizzata, deselezionare questa casella di controllo.

- ***Utilizza analisi euristica di AVG per rilevamento nuove reti***: consente di acquisire informazioni su una nuova rete rilevata con il metodo proprio di AVG (*questa opzione è disponibile solo su Windows Vista e versioni successive*).

- ***Utilizza analisi euristica di Microsoft per rilevamento nuove reti***: consente di acquisire informazioni su una nuova rete rilevata dal servizio Windows (*questa opzione è disponibile solo su Windows Vista e versioni successive*).

11.4. IDS

IDS (Intrusion Detection System) è una speciale funzionalità di analisi del comportamento progettata per identificare e bloccare tentativi di comunicazione sospetti su porte specifiche del computer. È possibile configurare i parametri IDS all'interno della finestra di dialogo ***Impostazioni IDS (Intrusion Detection System)***:

La finestra di dialogo ***Impostazioni IDS (Intrusion Detection System)*** offre le seguenti opzioni di configurazione:

- ***Blocca criminali informatici (attacchi port scanning e ARP) per un periodo di tempo definito***: consente di specificare per quanti secondi una porta deve essere bloccata ogni volta che viene rilevato un tentativo di comunicazione sospetto su tale porta. Per impostazione predefinita, l'intervallo di tempo è impostato su 1800 secondi (*30 minuti*).

- ***Blocca port scanning*** *(attivata per impostazione predefinita)*: selezionare questa casella per bloccare i tentativi di comunicazione su tutte le porte PCP e UDP che raggiungono il computer dall'esterno. Per ogni connessione di questo tipo, sono consentiti cinque tentativi e il sesto viene bloccato. Questa voce è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione. Se si mantiene attivata l'opzione ***Blocca port scanning***, è disponibile un'ulteriore opzione di configurazione dettagliata *(in caso contrario, la seguente voce sarà disattivata)*:

    - ***Scansione porte in blacklist***: selezionare questa casella per bloccare immediatamente qualsiasi tentativo di comunicazione sulle porte specificate nel campo di testo seguente. Le singole porte o gli intervalli di porte devono essere separati da virgole. Se si desidera utilizzare questa funzionalità, è disponibile un elenco predefinito di porte consigliate.

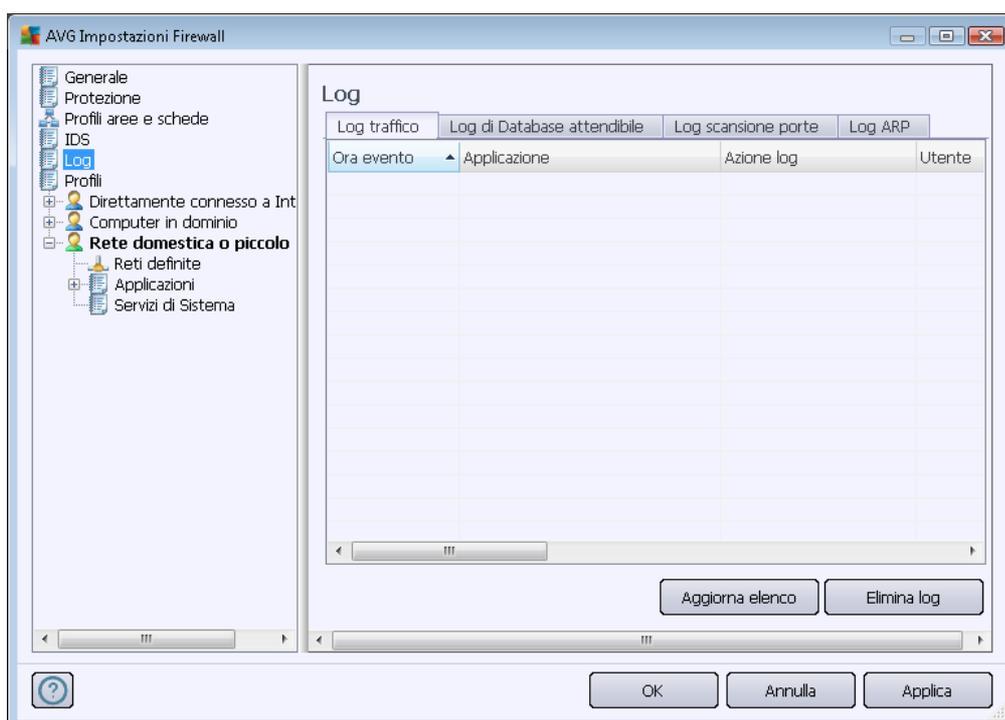
    - Attacchi bloccati: questa sezione elenca tutti i tentativi di comunicazione bloccati dal Firewall. La cronologia completa dei tentativi bloccati può essere visualizzata nella finestra di dialogo Log (*scheda Log scansione porte*).

- ***Blocca attacchi ARP (avanzato)*** *(disattivata per impostazione predefinita)*: selezionare questa opzione per attivare il blocco di tipi speciali di tentativi di comunicazione all'interno di

una rete locale rilevati da ***IDS*** come potenzialmente pericolosi. Viene applicata l'ora impostata in ***Blocca attacchi per un periodo di tempo definito***. È consigliabile che questa funzionalità venga utilizzata solo da utenti esperti, che conoscono il tipo e il livello di rischio della rete locale.

Pulsanti di controllo

- ***Aggiorna elenco***: selezionare il pulsante per aggiornare l'elenco (*in modo da includere gli eventuali tentativi bloccati più recenti*)
- ***Rimuovi***: selezionare per annullare un blocco selezionato
- ***Estendi timeout***: selezionare per prolungare il periodo di tempo per il quale un tentativo selezionato viene bloccato. Verrà visualizzata una nuova finestra di dialogo con opzioni estese che consentono di impostare data e ora specifiche o una durata illimitata.

11.5. Log

La finestra di dialogo ***Log*** consente di esaminare l'elenco di tutti gli eventi e le azioni Firewall registrati con una descrizione dettagliata dei relativi parametri (*ora dell'evento, nome dell'applicazione, rispettiva azione log, nome utente, PID, direzione del traffico, tipo di protocollo, numeri delle porte remote e locali e così via*) in quattro schede:

- ***Log traffico***: fornisce informazioni sull'attività di tutte le applicazioni che hanno tentato di connettersi alla rete.

- ***Log database attendibile***: il *database attendibile* è un database interno di AVG che raccoglie informazioni sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare in linea. La prima volta in cui una nuova applicazione tenta di connettersi alla rete (*ossia quando non è ancora stata specificata alcuna regola firewall per tale applicazione*), è necessario stabilire se la comunicazione di rete deve essere consentita per tale applicazione. Innanzitutto, AVG effettua una ricerca nel *database attendibile*. Se l'applicazione è elencata, sarà automaticamente autorizzata ad accedere alla rete. Se nel database non sono presenti informazioni sull'applicazione, verrà richiesto in una nuova finestra di dialogo se si desidera autorizzare l'applicazione ad accedere alla rete.

- ***Log scansione porte***: fornisce i log di tutte le attività di Intrusion Detection System.

- ***Log ARP***: log relativi al blocco di tipi speciali di tentativi di comunicazione all'interno di una rete locale (opzione *Blocca attacchi ARP*) rilevati da Intrusion Detection System come potenzialmente pericolosi.

Pulsanti di controllo

- ***Aggiorna elenco***: tutti i parametri registrati possono essere ordinati in base all'attributo selezionato: cronologicamente (*date*) o alfabeticamente (*altre colonne*). È sufficiente fare clic sull'intestazione di colonna pertinente. Utilizzare il pulsante ***Aggiorna elenco*** per aggiornare le informazioni visualizzate.

- ***Elimina log***: fare clic per eliminare tutte le voci presenti nel grafico.

11.6. Profili

Nella finestra di dialogo ***Impostazioni di profili*** è disponibile un elenco di tutti i profili disponibili:

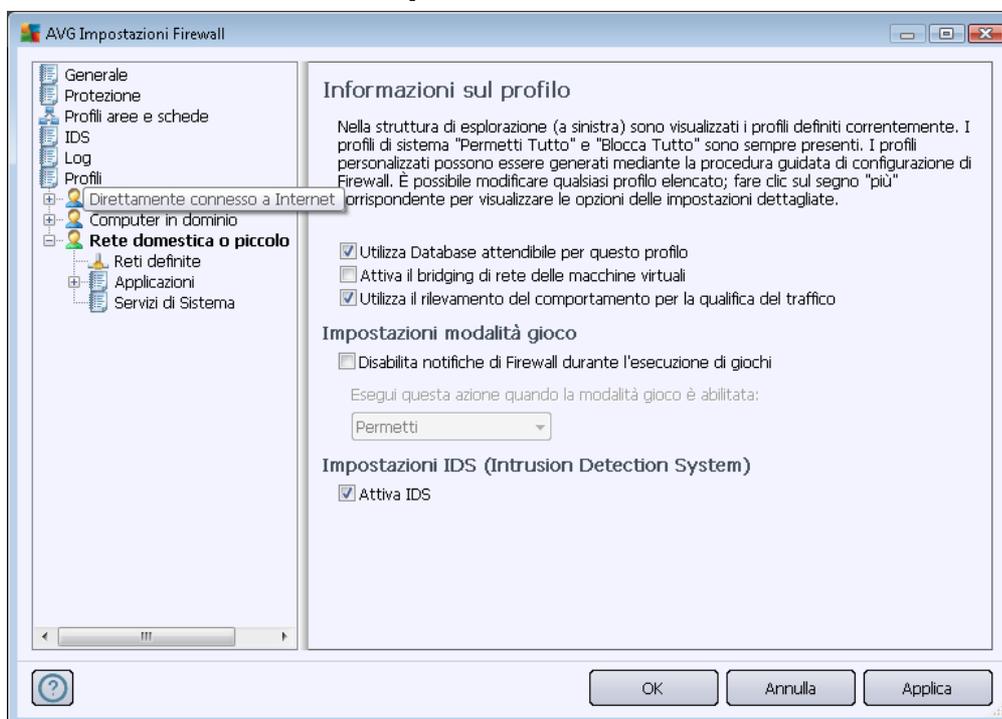
I profili di sistema *(Permetti Tutto, Blocca Tutto)* non sono modificabili. Tuttavia, tutti i profili personalizzati *(Direttamente connesso a Internet, Computer in dominio, Rete domestica o piccolo ufficio)* possono essere modificati in questa finestra di dialogo utilizzando i seguenti pulsanti di controllo:

- ***Attiva profilo***: questo pulsante consente di impostare il profilo selezionato come attivo. Significa che il profilo selezionato verrà utilizzato dal Firewall per controllare il traffico di rete.
- ***Duplica profilo***: consente di creare una copia identica del profilo selezionato. In seguito sarà possibile modificare e rinominare la copia per creare un nuovo profilo basato sull'originale duplicato.
- ***Rinomina profilo***: consente di definire un nuovo nome per il profilo selezionato.
- ***Elimina profilo***: consente di eliminare dall'elenco il profilo selezionato.
- ***Attiva/disattiva database attendibile***: per il profilo selezionato è possibile decidere di utilizzare le informazioni del *database attendibile* (*il database attendibile è un database interno di AVG che raccoglie dati sulle applicazioni certificate e attendibili che saranno sempre autorizzate a comunicare in linea).*).
- ***Esporta profilo***: consente di registrare la configurazione del profilo selezionato in un file che verrà salvato per un possibile ulteriore utilizzo.

- ***Importa profilo***: consente di configurare le impostazioni del profilo selezionato in base ai dati esportati dal file di configurazione di backup.

Nella sezione inferiore della finestra di dialogo si trova la descrizione del profilo attualmente selezionato nell'elenco.

Il menu di esplorazione visualizzato a sinistra cambierà in base al numero di profili definiti elencati nella finestra di dialogo ***Profilo***. Ogni profilo definito crea un ramo specifico sotto la voce ***Profilo***. È quindi possibile modificare specifici profili nelle seguenti finestre di dialogo (*che sono identiche per tutti i profili*):

11.6.1. Informazioni sui profili

La finestra di dialogo ***Informazioni sui profili*** è la prima di una sezione in cui è possibile modificare la configurazione di ogni profilo all'interno di diverse finestre separate relative a specifici parametri del profilo.

- ***Utilizza database attendibile per questo profilo*** (*attivata per impostazione predefinita*): selezionare questa opzione per attivare il *database attendibile* (*ossia il database interno di AVG che raccoglie informazioni sulle applicazioni certificate e attendibili che comunicano in linea. Se non è ancora stata specificata alcuna regola per un'applicazione, è necessario determinare se l'applicazione può essere autorizzata ad accedere alla rete. AVG effettua innanzitutto una ricerca nel database attendibile. Se l'applicazione è elencata, sarà considerata sicura e autorizzata a comunicare sulla rete. Altrimenti, l'utente dovrà specificare se l'applicazione deve essere autorizzata a comunicare sulla rete*) per il rispettivo profilo

- ***Attiva il bridging di rete delle macchine virtuali*** (*disattivata per impostazione predefinita*

): selezionare questa voce per consentire alle macchine virtuali in VMware di connettersi direttamente alla rete.

- ***Utilizza il rilevamento del comportamento per la qualifica del traffico*** (*attivata per impostazione predefinita*): selezionare questa opzione per consentire al componente Firewall di utilizzare la funzionalità Identity Protection per la valutazione di un'applicazione. Identity Protection è in grado di determinare se l'applicazione mostra un comportamento sospetto oppure è attendibile e può comunicare in linea.

Impostazioni modalità gioco

Nella sezione ***Impostazioni modalità gioco*** è possibile decidere, e confermare selezionando la rispettiva voce, se si desidera che vengano visualizzati messaggi informativi del Firewall anche quando è in esecuzione un'applicazione a schermo intero sul computer (*in genere si tratta di giochi, ma l'impostazione si applica a qualunque applicazione a schermo intero, ad esempio le presentazioni in formato PPT*), poiché i messaggi informativi possono in qualche modo interferire con l'attività svolta.

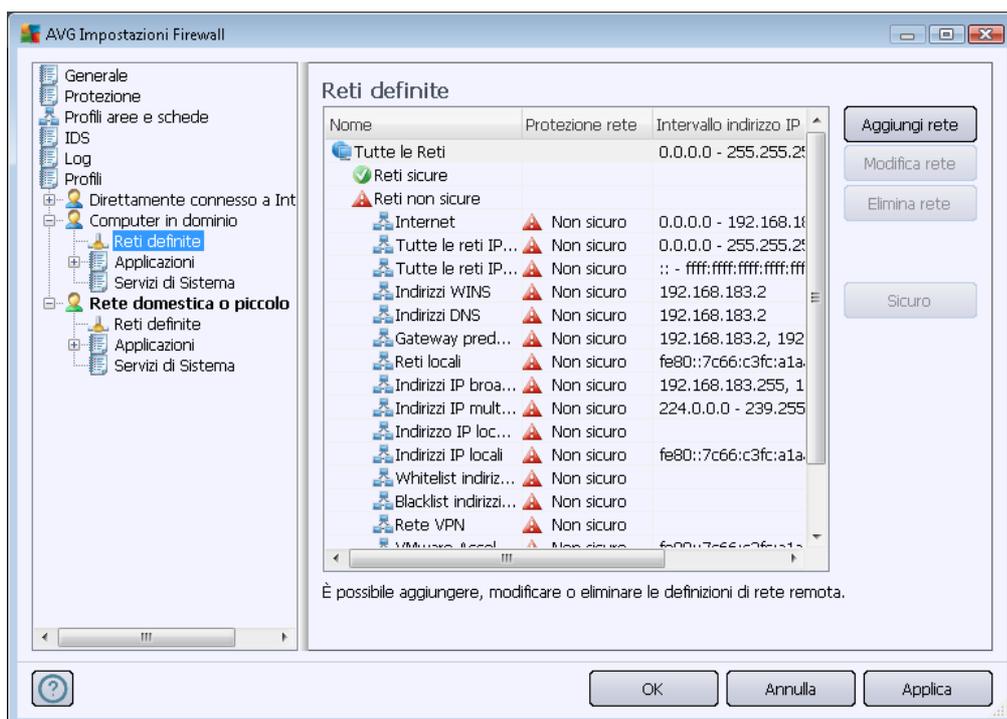
Se si seleziona la voce ***Disabilita notifiche di Firewall durante l'esecuzione di giochi***, è necessario selezionare nel menu a discesa quale azione deve essere eseguita qualora una nuova applicazione ancora priva di regole specificate tenti di comunicare in rete (*applicazioni per cui normalmente verrebbe visualizzata una finestra di richiesta di conferma*). Tutte queste applicazioni possono essere consentite o bloccate.

Se la modalità gioco è attivata, tutte le attività pianificate (*scansioni e aggiornamenti*) vengono posticipate finché l'applicazione non viene chiusa.

Impostazioni IDS (Intrusion Detection System)

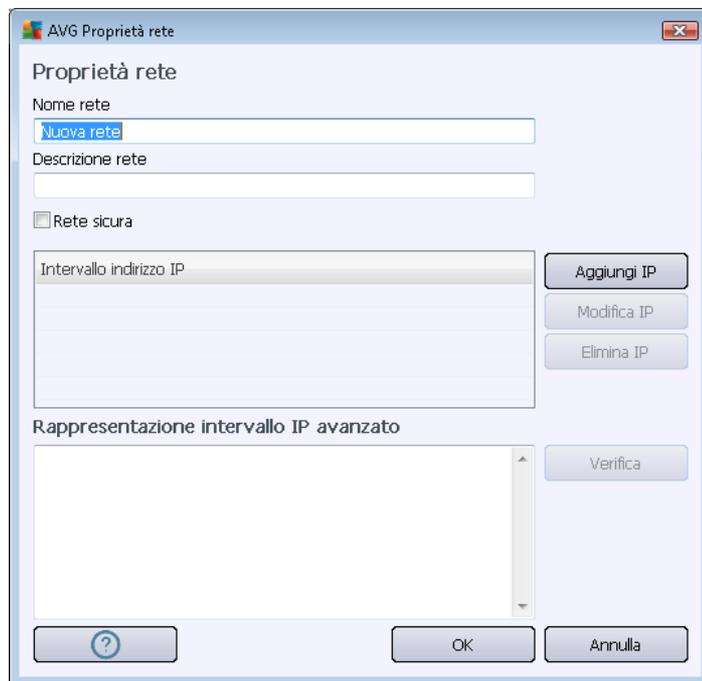
Selezionare la casella ***Abilita IDS*** per attivare una speciale funzionalità di analisi del comportamento progettata per identificare e bloccare tentativi di comunicazione sospetti su porte specifiche del computer *(per dettagli sulle impostazioni di questa funzionalità consultare il capitolo relativo a IDS di questo documento).*

11.6.2. Reti definite

Nella finestra di dialogo ***Reti definite*** è disponibile un elenco di tutte le reti a cui è connesso il computer.

L'elenco fornisce le seguenti informazioni su ciascuna rete rilevata:

- ***Reti***: fornisce l'elenco dei nomi di tutte le reti a cui è connesso il computer.
- ***Protezione rete***: per impostazione predefinita, tutte le reti vengono considerate non sicure e solo se si è certi che una rete sia sicura è possibile contrassegnarla come tale (*fare clic sulla voce di elenco relativa alla rete desiderata e selezionare Sicuro dal menu di scelta rapida*). Tutte le reti sicure verranno quindi incluse nel gruppo delle reti attraverso le quali l'applicazione potrà comunicare con la regola dell'applicazione impostata su Consenti protette.
- ***Intervallo indirizzi IP***: ogni rete verrà rilevata automaticamente e specificata sotto forma di intervallo di indirizzi IP.

Pulsanti di controllo

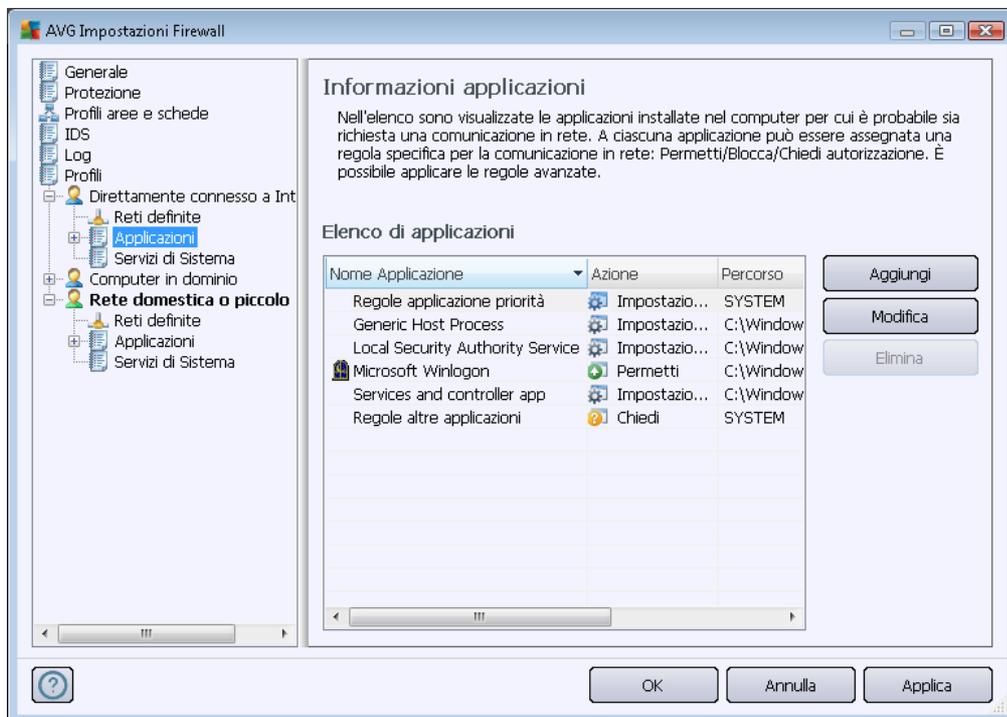
- ***Aggiungi rete***: consente di aprire la finestra di dialogo ***Proprietà rete*** in cui è possibile modificare i parametri della rete appena definita:

In questa finestra di dialogo è possibile specificare il ***Nome rete***, fornire la ***Descrizione rete*** ed eventualmente contrassegnare la rete come sicura. La nuova rete può essere definita manualmente in una finestra di dialogo autonoma aperta mediante il pulsante ***Aggiungi IP*** (in alternativa ***Modifica IP*** / ***Elimina IP***). In questa finestra di dialogo è possibile specificare la rete mediante la relativa maschera o il relativo intervallo IP. Per un grande numero di reti da definire come parte della rete appena creata è possibile utilizzare l'opzione ***Rappresentazione intervallo IP avanzato***: immettere l'elenco di tutte le reti nel relativo campo di testo (*è supportato qualunque formato standard*) e selezionare il pulsante ***Verifica*** per assicurarsi che il formato possa essere riconosciuto. Quindi selezionare ***OK*** per confermare e salvare i dati.

- ***Modifica rete***: consente di aprire la finestra di dialogo ***Proprietà rete*** (*vedere sopra*) in cui è possibile modificare i parametri di una rete già definita (*questa finestra di dialogo è identica alla finestra di dialogo per l'aggiunta di nuove reti; vedere la descrizione nel paragrafo precedente*).

- ***Elimina rete***: consente di rimuovere il nodo di una rete selezionata dall'elenco delle reti.

- ***Segna come sicuro***: per impostazione predefinita, tutte le reti vengono considerate non sicure e solo se si è certi che una rete sia sicura è possibile utilizzare questo pulsante per contrassegnarla come tale (*viceversa, una volta che la rete è stata contrassegnata come sicura, il testo del pulsante viene modificato in "Segna come non sicuro"*).

11.6.3. Applicazioni

Nella finestra di dialogo ***Informazioni applicazioni*** sono elencate tutte le applicazioni installate per cui potrebbe essere necessario stabilire una comunicazione in rete e le icone per l'azione assegnata:

Le applicazioni visualizzate in ***Elenco di applicazioni*** sono state rilevate sul computer (*e dispongono delle rispettive azioni assegnate*). È possibile utilizzare i seguenti tipi di azione:

- - Consenti comunicazione per tutte le reti
- - Consenti comunicazione solo per reti definite come sicure
- - Blocca comunicazione
- - Visualizza finestra di dialogo di conferma (*l'utente potrà decidere se consentire o bloccare la comunicazione quando l'applicazione tenterà di comunicare sulla rete*)
- - Impostazioni avanzate definite

Tenere presente che è possibile rilevare solo le applicazioni già installate, pertanto se si installa una nuova applicazione in un secondo momento sarà necessario definire le relative regole Firewall. Per impostazione predefinita, quando la nuova applicazione tenta di connettersi in rete per la prima volta, il firewall crea automaticamente una regola in base al Database attendibile oppure chiede all'utente se consentire o bloccare la comunicazione. Nel secondo caso, sarà possibile salvare la risposta come regola permanente (che verrà quindi elencata in questa finestra di dialogo).

Naturalmente, è anche possibile definire immediatamente le regole per la nuova applicazione. In questa finestra di dialogo fare clic su ***Aggiungi*** e immettere i dettagli richiesti.

Oltre alle applicazioni, nell'elenco sono incluse anche due voci speciali:

- ***Regole per applicazione prioritaria*** (*nella parte superiore dell'elenco*). Queste regole sono

preferenziali e vengono sempre applicate prima delle regole di ogni singola applicazione.

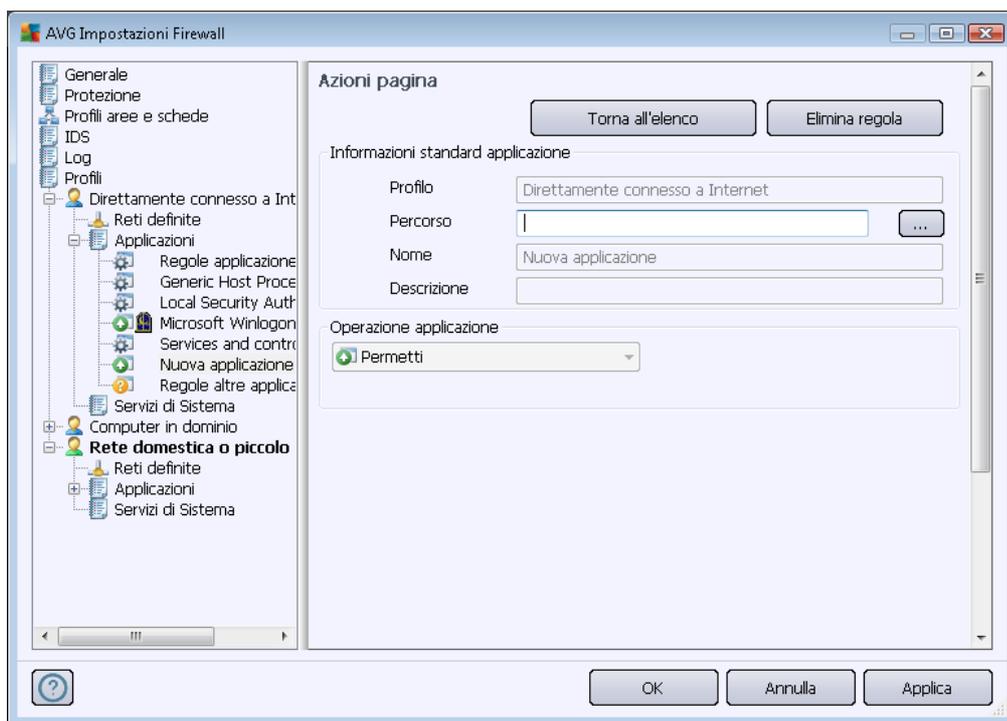
- ***Regole per altre applicazioni*** (*nella parte inferiore dell'elenco*). Queste regole sono utilizzate come "ultima istanza" quando non si applicano regole di applicazioni specifiche, ad esempio per un'applicazione sconosciuta e non definita. Selezionare l'azione che deve essere attivata se tale applicazione effettuasse un tentativo di comunicazione sulla rete:
  - *Blocca*: la comunicazione sarà sempre bloccata.
  - *Consenti*: la comunicazione sarà consentita su tutte le reti.
  - *Chiedi* : l'utente dovrà specificare se la comunicazione deve essere consentita o bloccata.

Questi elementi presentano opzioni di impostazione diverse dalle applicazioni comuni e sono destinati esclusivamente agli utenti esperti. Si consiglia di non modificare le impostazioni.

Pulsanti di controllo

Per modificare l'elenco, utilizzare i seguenti pulsanti di controllo:

- ***Aggiungi***: consente di aprire una finestra di dialogo Azioni pagina vuota per la definizione di regole per una nuova applicazione.
- ***Modifica***: consente di aprire la stessa finestra di dialogo Azioni pagina completa di dati per la modifica di un insieme di regole per un'applicazione esistente.
- ***Elimina***: consente di rimuovere dall'elenco l'applicazione selezionata.

Nella finestra di dialogo ***Azioni pagina*** è possibile definire le impostazioni dettagliate per la rispettiva applicazione:

Pulsanti di controllo

Due pulsanti di controllo sono disponibili nella parte superiore della finestra di dialogo:

- ***Torna all'elenco***: fare clic su questo pulsante per visualizzare la panoramica di tutte le regole delle applicazioni definite.
- ***Elimina regola***: fare clic su questo pulsante per eliminare la regola dell'applicazione visualizzata. ***Tenere presente che l'azione non può essere annullata.***

Informazioni standard applicazione

In questa sezione immettere il ***nome*** dell'applicazione e, facoltativamente, una ***descrizione*** (*un breve commento per informazione personale*). Nel campo ***Percorso*** immettere il percorso completo dell'applicazione (*il file eseguibile*) sul disco. In alternativa, è possibile individuare l'applicazione nella struttura facendo clic sul pulsante "***...***".

Operazione applicazione

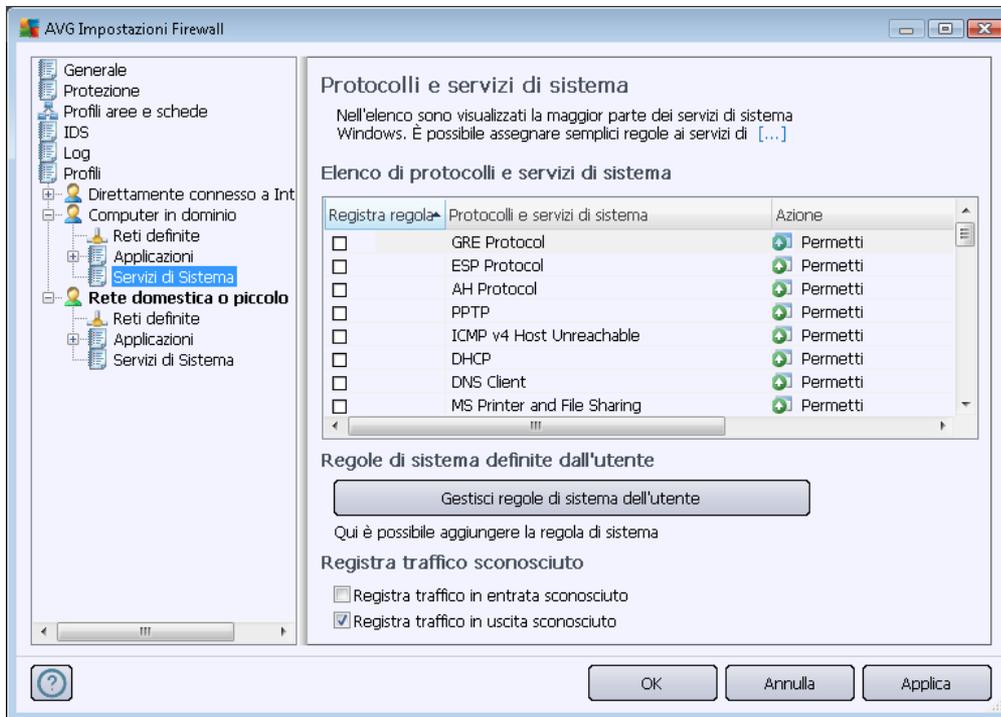
Dal menu a discesa è possibile scegliere la regola Firewall per l'applicazione, ovvero scegliere le

operazioni che si desidera vengano eseguite dal componente Firewall quando l'applicazione tenta di stabilire una comunicazione in rete:

- ***Consenti tutte***: consente all'applicazione di comunicare su tutte le reti e le schede definite, senza limiti.
- ***Consenti protette***: consente all'applicazione di comunicare solo su reti definite come sicure *(affidabili)*.
- ***Blocca***: impedisce la comunicazione automaticamente; l'applicazione non potrà eseguire la connessione a nessuna rete.
- ***Chiedi***: visualizza una finestra di dialogo che permette di scegliere se si desidera consentire o bloccare il tentativo di stabilire una comunicazione.
- ***Impostazioni avanzate***: visualizza ulteriori opzioni di impostazione complete e dettagliate nella parte inferiore della finestra di dialogo della sezione ***Regole dettagli applicazione***. I dettagli verranno applicati in base all'ordine in cui sono elencati, pertanto è possibile ***spostare su*** o ***spostare giù*** le regole all'interno dell'elenco in base alle necessità per impostarne la precedenza. Dopo aver fatto clic su una specifica regola dell'elenco, la panoramica dei dettagli della regola viene visualizzata nella parte inferiore della finestra di dialogo. Tutti i valori sottolineati in blu possono essere modificati tramite clic nella rispettiva finestra di dialogo relativa alle impostazioni. Per eliminare la regola evidenziata, fare clic su ***Rimuovi***. Per definire una nuova regola, utilizzare il pulsante ***Aggiungi*** per aprire la finestra di dialogo ***Modifica dettaglio*** che consente di specificare tutti i dettagli necessari.

11.6.4. Servizi di sistema

Le modifiche alla finestra di dialogo Protocolli e servizi di sistema sono riservate ESCLUSIVAMENTE agli UTENTI ESPERTI.

La finestra di dialogo ***Protocolli e servizi di sistema*** elenca i protocolli e i servizi di sistema standard di Windows che potrebbero dover comunicare sulla rete:

Elenco di protocolli e servizi di sistema

Il grafico presenta le seguenti colonne:

- ***Registra azione regola***: questa casella consente di attivare la registrazione di ciascuna applicazione della regola nei log.
- ***Protocolli e servizi di sistema***: questa colonna mostra il nome del rispettivo servizio di sistema.
- ***Azione***: questa colonna mostra un'icona per l'azione assegnata:
  - Consenti comunicazione per tutte le reti
  - Consenti comunicazione solo per reti definite come sicure
  - Blocca comunicazione
- ***Reti***: questa colonna indica a quale rete si riferisce la regola di sistema.

Per modificare le impostazioni delle voci dell'elenco (*incluse le azioni assegnate*), fare clic con il pulsante destro del mouse sulla voce desiderata e selezionare ***Modifica***. ***La modifica delle regole di sistema può essere eseguita solo da utenti avanzati. È consigliabile non modificare le regole di sistema.***

Regole di sistema definite dall'utente

Per aprire una nuova finestra di dialogo per la definizione di una regola dei servizi di sistema personalizzata (*vedere la seguente immagine*), selezionare il pulsante ***Gestisci regole di sistema dell'utente***. La sezione superiore della finestra di dialogo ***Regole di sistema definite dall'utente*** visualizza una panoramica di tutti i dettagli della regola di sistema modificata; la sezione inferiore visualizza quindi il dettaglio selezionato. I dettagli delle regole definite dall'utente possono essere modificati, aggiunti o eliminati tramite gli appositi pulsanti; i dettagli delle regole definite dal produttore possono essere solo modificati:

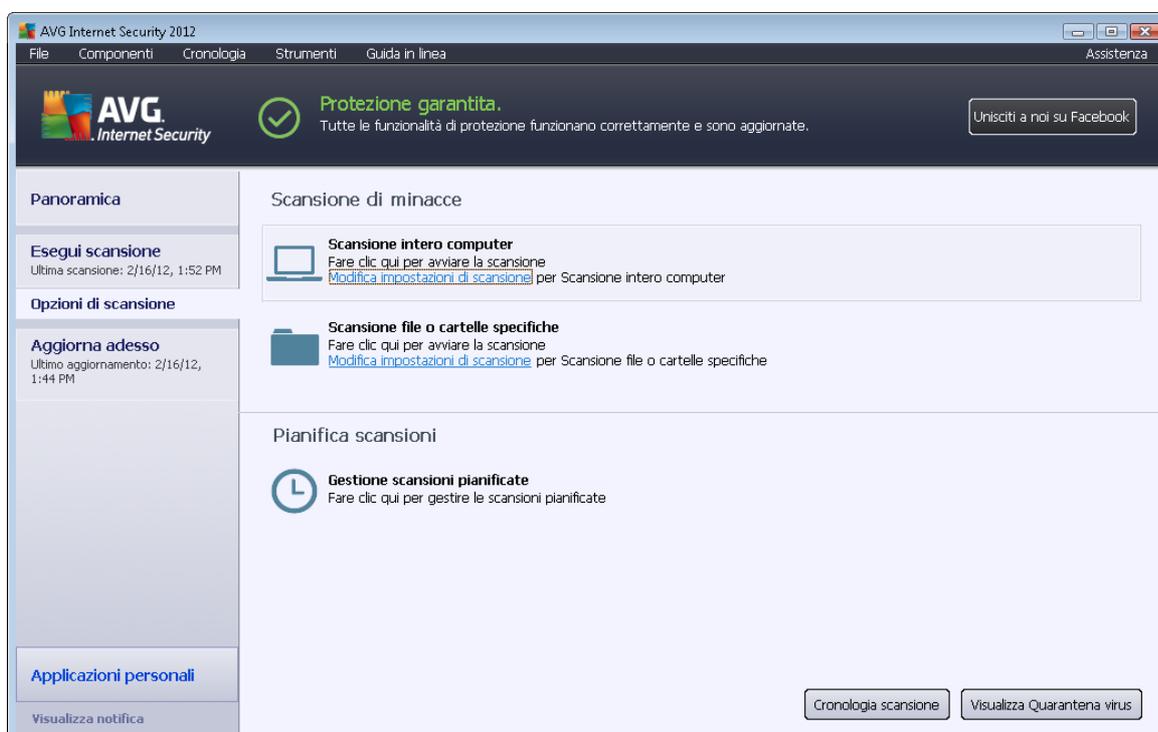
Tenere presente che queste impostazioni delle regole dettagliate sono avanzate e destinate innanzitutto agli amministratori di rete che necessitano del controllo completo della configurazione del componente Firewall. Se non si conoscono i tipi di protocollo di comunicazione, i numeri delle porte di rete, le definizioni degli indirizzi IP e così via, non modificare queste impostazioni. Se fosse necessario modificare la configurazione, consultare i file della Guida della rispettiva finestra di dialogo per dettagli specifici.

Registra traffico sconosciuto

- ***Registra traffico in entrata sconosciuto*** *(disattivata per impostazione predefinita)*: selezionare la casella per registrare nei Log ciascun tentativo sconosciuto di connessione al computer dall'esterno.
- ***Registra traffico in uscita sconosciuto*** *(attivata per impostazione predefinita)*: selezionare la casella per registrare nei Log ciascun tentativo sconosciuto del computer di connettersi a una posizione esterna.

12. Scansione AVG

Per impostazione predefinita, **AVG Internet Security 2012** non esegue alcuna scansione, poiché dopo la scansione iniziale il computer dovrebbe essere perfettamente protetto dai componenti permanenti di **AVG Internet Security 2012** che sono sempre in guardia e non lasciano entrare codice dannoso nel sistema. Naturalmente, è possibile pianificare l'esecuzione di una scansione a intervalli regolari o avviare manualmente una scansione in qualsiasi momento in base alle esigenze.

12.1. Interfaccia di scansione

L'interfaccia di scansione di AVG è accessibile tramite il collegamento rapido ***Opzioni di scansione*** . Fare clic sul collegamento per accedere alla finestra di dialogo ***Scansione di minacce***. Nella finestra di dialogo è contenuto quanto segue:

- panoramica delle scansioni predefinite: sono disponibili tre tipi di scansione definiti dal fornitore del software che possono essere utilizzati immediatamente su richiesta oppure pianificati:
    - Scansione intero computer
    - Scansione file o cartelle
- sezione Pianificazione scansioni, dove si possono definire nuovi controlli e creare nuove pianificazioni in base alle esigenze.

Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di controllo sono i seguenti:

- ***Cronologia scansione*** : consente di visualizzare la finestra di dialogo Panoramica risultati di scansione insieme alla cronologia completa della scansione
- ***Visualizza Quarantena virus***: consente di aprire una nuova finestra con Quarantena virus, lo spazio in cui le infezioni rilevate vengono messe in quarantena

12.2. Scansioni predefinite

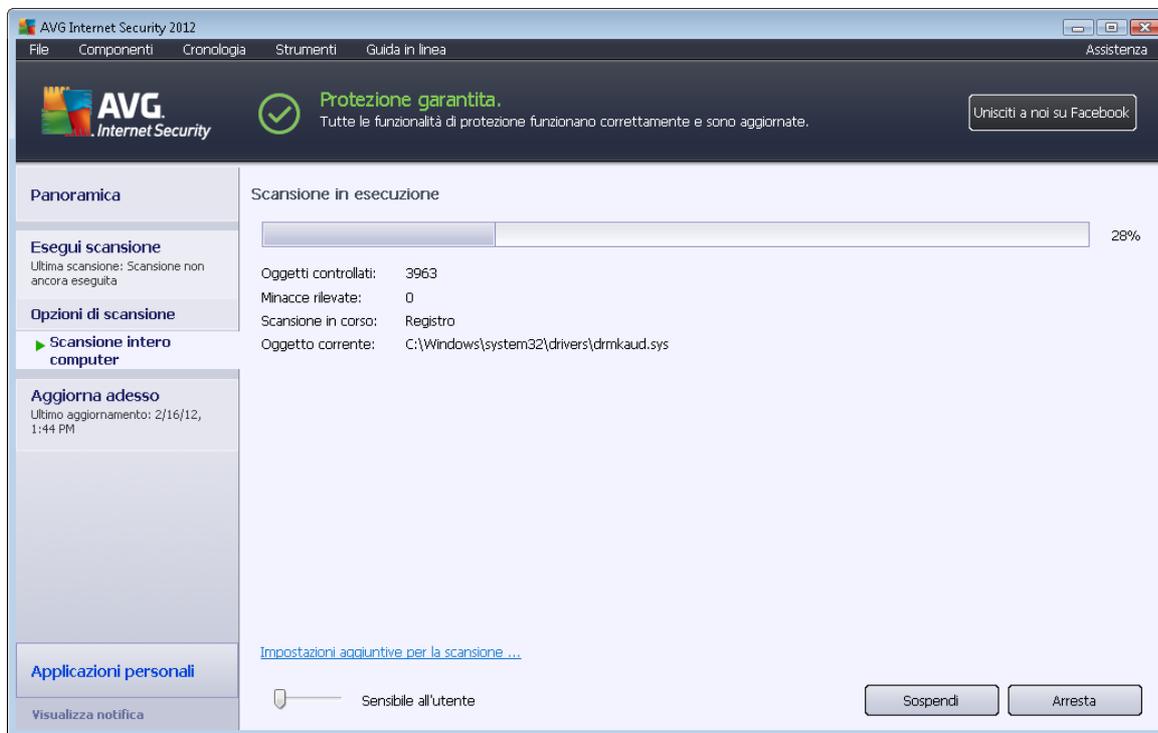
Una delle funzioni principali di **AVG Internet Security 2012** è la scansione su richiesta. I controlli su richiesta sono progettati per eseguire la scansione di varie parti del computer quando si sospetta una possibile infezione da virus. Comunque, si consiglia di eseguire regolarmente tali verifiche anche se non si ritiene che siano presenti virus nel computer.

In **AVG Internet Security 2012** sono disponibili i seguenti tipi di scansione predefiniti dal fornitore del software:

12.2.1. Scansione intero computer

Scansione intero computer: consente di eseguire la scansione dell'intero computer per il rilevamento di possibili infezioni e/o di programmi potenzialmente indesiderati. Questo controllo eseguirà la scansione di tutti i dischi rigidi del computer, rileverà e correggerà i virus trovati oppure sposterà l'infezione rilevata in Quarantena virus. È necessario pianificare la scansione completa di una workstation almeno una volta la settimana.

Avvio della scansione

È possibile avviare la ***Scansione intero computer*** direttamente dall'interfaccia di scansione facendo clic sull'icona di scansione. Non è necessario configurare ulteriori impostazioni specifiche per questo tipo di scansione. La scansione verrà avviata immediatamente nella finestra di dialogo ***Scansione in esecuzione*** (*vedere la schermata*). La scansione può essere temporaneamente interrotta (***Sospendi***) oppure annullata (***Arresta***) se necessario.

Modifica della configurazione della scansione

È possibile modificare le impostazioni predefinite di ***Scansione intero computer***. Selezionare il collegamento ***Modifica impostazioni di scansione*** per accedere alla finestra di dialogo ***Modifica impostazioni di scansione per Scansione intero computer*** *(accessibile dall'interfaccia di scansione tramite il collegamento Modifica impostazioni di scansione per Scansione intero computer)*. ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

- ***Parametri scansione***: dall'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:
  - ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** (*attivata per impostazione predefinita*): se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.
  - ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
  - ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
  - ***Scansione cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro del componente Anti-Spyware stabilisce che i cookie devono essere

rilevati (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*).

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quale ZIP, RAR e così via.
- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.
- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- ***Ricerca di rookit*** (*attivata per impostazione predefinita*): la scansione Anti-Rootkit cerca nel computer possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:

- *Opzioni arresto computer*: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

- ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

  - ***Tutti i tipi di file*** con la possibilità di definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

  - Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente per l'utilizzo automatico delle risorse.* In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare:

Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione definita, come descritto nel capitolo* *Scansione AVG / Pianificazione di scansioni / Scansione da eseguire*. *Se si decide di modificare la configurazione predefinita di* **Scansione intero computer** *, è possibile salvare le nuove impostazioni come configurazione predefinita da utilizzare per tutte le altre scansioni dell'intero computer.*

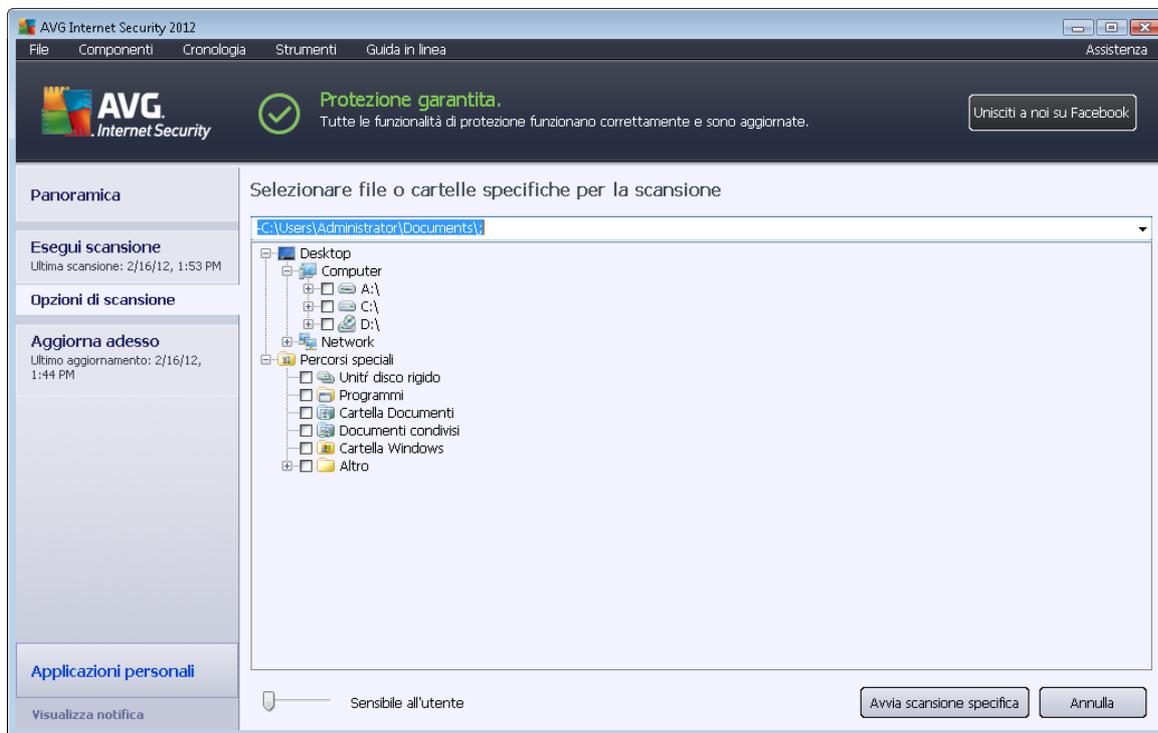
12.2.2. Scansione file o cartelle

Scansione file o cartelle: consente di eseguire la scansione delle sole aree del computer selezionate per la scansione (*cartelle, dischi rigidi, dischi floppy, CD selezionati e così via*). L'avanzamento della scansione nel caso di rilevamento di virus e relativo trattamento è uguale a quello della scansione dell'intero computer: gli eventuali virus rilevati vengono corretti o spostati in Quarantena virus. La scansione di file o cartelle specifiche può essere utilizzata per impostare controlli personalizzati e la relativa pianificazione in base alle esigenze.

Avvio della scansione

È possibile avviare ***Scansione file o cartelle*** direttamente dall'interfaccia di scansione facendo clic sull'icona di scansione. Viene aperta una nuova finestra di dialogo ***Selezionare file o cartelle specifiche per la scansione***. Nella struttura del computer selezionare le cartelle che si desidera sottoporre a scansione. Il percorso di ciascuna cartella selezionata verrà generato automaticamente e visualizzato nella casella di testo nella parte superiore della finestra di dialogo.

È possibile sottoporre a scansione una specifica cartella escludendo tutte le sottocartelle relative; a questo scopo scrivere un segno meno "**-**" davanti al percorso generato automaticamente (*vedere la schermata*). Per escludere l'intera cartella dalla scansione, utilizzare il parametro "!".

Infine, per avviare la scansione, selezionare il pulsante ***Avvia scansione***; il processo di scansione è praticamente identico a quello della scansione dell'intero computer.

Modifica della configurazione della scansione

È possibile modificare le impostazioni predefinite di ***Scansione file o cartelle***. Selezionare il collegamento ***Modifica impostazioni di scansione*** per accedere alla finestra di dialogo ***Modifica impostazioni di scansione per Scansione file o cartelle***. ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

- ***Parametri scansione***: dall'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

  - ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** (*attivata per impostazione predefinita*): se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

  - ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

  - ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

  - ***Scansione cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro del componente Anti-Spyware stabilisce che i cookie devono essere

rilevati (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*).

- ***Scansione all'interno degli archivi*** (*attivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche quelli inclusi all'interno di un archivio, quale ZIP, RAR e così via

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*disattivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:

- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

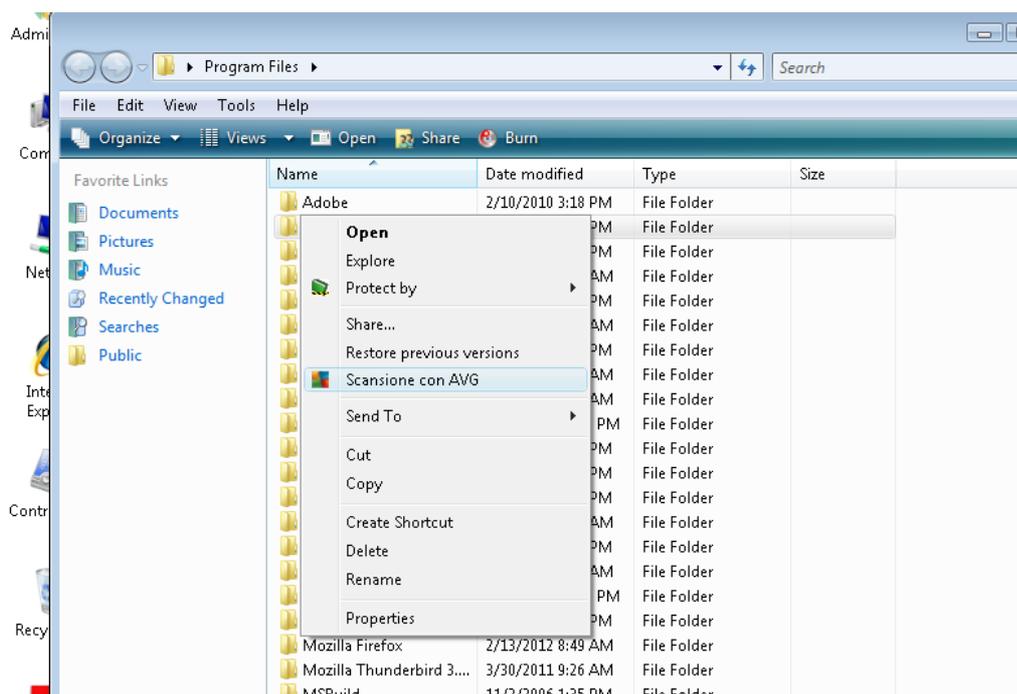
- *Tipi di file per la scansione*: specificare se si desidera sottoporre a scansione:
  - ***Tutti i tipi di file*** con la possibilità di definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;
  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.
  - Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

- ***Priorità processi di scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente per l'utilizzo automatico delle risorse.* In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare:

Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione definita, come descritto nel capitolo [Scansione AVG / Pianificazione di scansioni / Scansione da eseguire](). Se si decide di modificare la configurazione predefinita di* ***Scansione file o cartelle*** *è possibile salvare la nuova impostazione come configurazione predefinita da utilizzare per tutte le altre scansioni di file o cartelle specifiche. Inoltre, questa configurazione verrà utilizzata come modello per tutte le nuove scansioni pianificate ([tutte le scansioni personalizzate si basano sulla configurazione corrente di Scansione file o cartelle]()).*

12.3. Scansione in Esplora risorse

Oltre alle scansioni predefinite avviate per l'intero computer o per le aree selezionate, **AVG Internet Security 2012** offre l'opzione di scansione rapida di un oggetto specifico direttamente nell'ambiente Esplora risorse. Se si desidera aprire un file sconosciuto e non si è sicuri del contenuto, è possibile decidere di eseguire un controllo su richiesta. Procedere come segue:

- In Esplora risorse evidenziare il file *o la cartella* che si desidera verificare
- Fare clic con il pulsante destro del mouse sull'oggetto per aprire il menu di scelta rapida
- Selezionare l'opzione ***Scansione con AVG*** per eseguire la scansione con **AVG Internet Security 2012**

12.4. Scansione da riga di comando

In **AVG Internet Security 2012** è possibile eseguire la scansione dalla riga di comando. Ad esempio, è possibile utilizzare questa opzione sui server oppure durante la creazione di uno script batch da avviare automaticamente dopo l'avvio del computer. Dalla riga di comando è possibile avviare la scansione con la maggior parte dei parametri forniti nell'interfaccia utente grafica di AVG.

Per avviare la scansione AVG dalla riga di comando, eseguire il seguente comando dalla cartella in cui è stato installato AVG:

- ***avgscanx*** per sistemi operativi a 32 bit
- ***avgscana*** per sistemi operativi a 64 bit

Sintassi del comando

La sintassi del comando è la seguente:

- ***avgscanx /parametro*** ... ad esempio ***avgscanx /comp*** per la scansione dell'intero computer
- ***avgscanx /parametro /parametro*** .. nel caso di più parametri, questi devono essere allineati in una riga e separati da uno spazio e dal carattere della barra (/)
- se per un parametro è necessario fornire un valore specifico (ad esempio, il parametro ***/scan*** richiede informazioni relative alle aree del computer di cui eseguire la scansione ed è necessario fornire il percorso esatto della sezione selezionata), i valori vengono separati da punto e virgola. Ad esempio: ***avgscanx /scan=C:\;D:***

Parametri di scansione

Per visualizzare una panoramica completa dei parametri disponibili, digitare il rispettivo comando insieme al parametro /? o /HELP (ad esempio ***avgscanx /?***). Nota: l'unico parametro obbligatorio è /SCAN, che consente di specificare quali aree del computer devono essere sottoposte a scansione. Per spiegazioni più dettagliate delle opzioni, vedere la panoramica dei parametri da riga di comando.

Per eseguire la scansione, premere ***Invio***. Durante la scansione è possibile arrestare il processo premendo ***Ctrl+C*** oppure ***Ctrl+Pausa***.

Scansione CMD avviata dall'interfaccia grafica

Quando viene eseguita la modalità provvisoria di Windows, è inoltre possibile avviare la scansione da riga di comando dall'interfaccia utente grafica. La scansione verrà avviata dalla riga di comando. La finestra di dialogo ***Compositore riga di comando*** consente solo di specificare la maggior parte dei parametri di scansione nella comoda interfaccia grafica.

Poiché questa finestra di dialogo è accessibile solo nella modalità provvisoria di Windows, per ulteriori informazioni consultare il file della Guida aperto direttamente dalla finestra di dialogo.

12.4.1. Parametri scansione CMD

Di seguito viene fornito un elenco di tutti i parametri disponibili per la scansione dalla riga di comando:

- ***/SCAN*** Scansione file o cartelle /SCAN=percorso;percorso *(ad esempio /SCAN=C:\;D:\)*
- ***/COMP*** Scansione intero computer
- ***/HEUR*** Usa analisi euristica

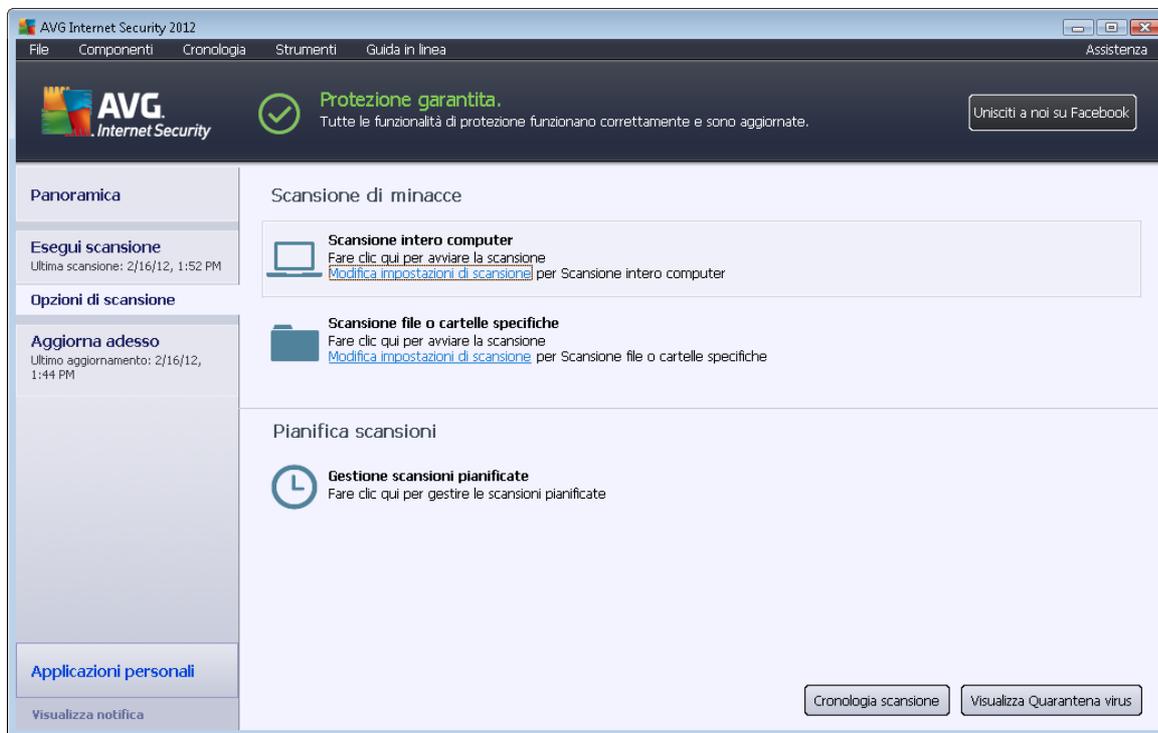
- ***/EXCLUDE*** Escludi percorso o file dalla scansione
- ***/@*** File di comando /nome file/
- ***/EXT*** Esegui scansione su queste estensioni /ad esempio EXT=EXE, DLL/
- ***/NOEXT*** Non eseguire scansione su queste estensioni /ad esempio NOEXT=JPG/
- ***/ARC*** Esegui scansione su archivi
- ***/CLEAN*** Pulisci automaticamente
- ***/TRASH*** Sposta file infetti in Quarantena virus
- ***/QT*** Controllo rapido
- ***/LOG*** Genera file risultati scansione
- ***/MACROW*** Segnala macro
- ***/PWDW*** Rapporto sui file protetti da password
- ***/ARCBOMBSW*** Segnala bombe a decompressione *(archivi compressi più volte)*
- ***/IGNLOCKED*** Ignora file bloccati
- ***/REPORT*** Rapporto sul file /nome file/
- ***/REPAPPEND*** Allega al file rapporto
- ***/REPOK*** Segnala file non infetti come OK
- ***/NOBREAK*** Non consentire interruzione CTRL-BREAK
- ***/BOOT*** Abilita controllo MBR/BOOT
- ***/PROC*** Scansione dei processi attivi
- ***/PUP*** Segnala i programmi potenzialmente indesiderati
- ***/PUPEXT*** Segnala set potenziati di programmi potenzialmente indesiderati
- ***/REG*** Scansione Registro di sistema
- ***/COO*** Esegui scansione dei cookie
- ***/?*** Visualizza la Guida sull'argomento
- ***/HELP*** Visualizza la Guida sull'argomento

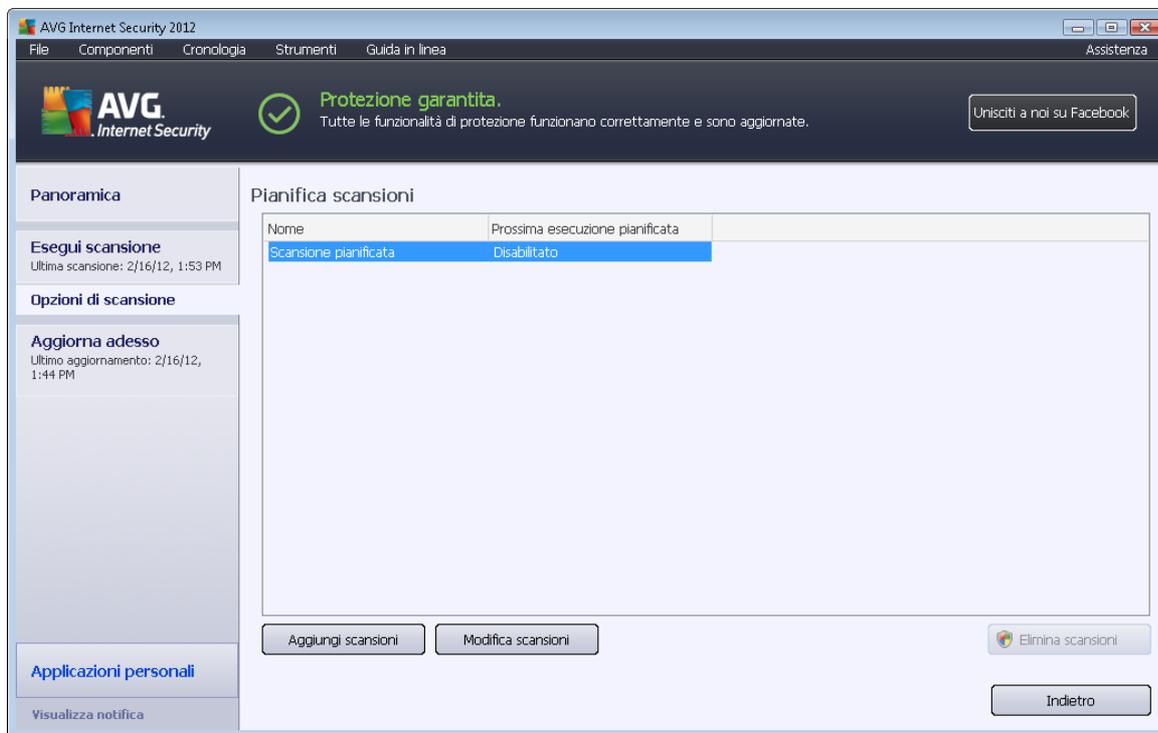
- ***/PRIORITY*** Imposta priorità scansione /bassa, automatica, alta/ *(vedere [Impostazioni avanzate / Scansioni](#))*
- ***/SHUTDOWN*** Arresta computer al completamento della scansione
- ***/FORCESHUTDOWN*** Forza arresto del computer al completamento della scansione
- ***/ADS*** Esegui scansione flussi di dati alternativi *(solo NTFS)*
- ***/HIDDEN*** Segnala i file con estensione nascosta
- ***/INFECTABLEONLY*** Scansione dei soli file con estensioni infettabili
- ***/THOROUGHSCAN*** Attiva scansione completa
- ***/CLOUDCHECK*** Ricerca di falsi positivi
- ***/ARCBOMBSW*** Segnala file di archivio ricompressi

12.5. Pianificazione di scansioni

AVG Internet Security 2012 consente di eseguire scansioni su richiesta (ad esempio quando si sospetta che un'infezione sia stata trasferita nel computer) oppure in base a una pianificazione. Si consiglia di eseguire le scansioni in base a una pianificazione: in questo modo ci si assicura che il computer sia protetto da possibili infezioni e non è necessario preoccuparsi dell'avvio della scansione.

Scansione intero computer deve essere avviata regolarmente, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, è possibile pianificare le scansioni fuori dagli orari di lavoro. Se il computer rimane a volte spento, è possibile pianificare l'esecuzione delle scansioni all'avvio del computer, nel caso in cui l'attività non sia stata eseguita.

Per creare nuove pianificazioni di scansioni, vedere l'interfaccia di scansione di AVG e individuare la sezione inferiore denominata ***Pianificazione scansioni***:

Pianificazione scansioni

Fare clic sull'icona grafica all'interno della sezione ***Pianificazione scansioni*** per aprire una nuova finestra di dialogo ***Pianificazione scansioni*** in cui è disponibile un elenco di tutte le scansioni pianificate al momento:

È possibile modificare / aggiungere scansioni utilizzando i seguenti pulsanti di controllo:

- ***Aggiungi pianificazione scansione***: il pulsante consente di aprire la finestra di dialogo ***Impostazioni per scansione pianificata***, scheda Impostazioni pianificazione. In questa finestra di dialogo è possibile specificare i parametri del nuovo controllo definito.

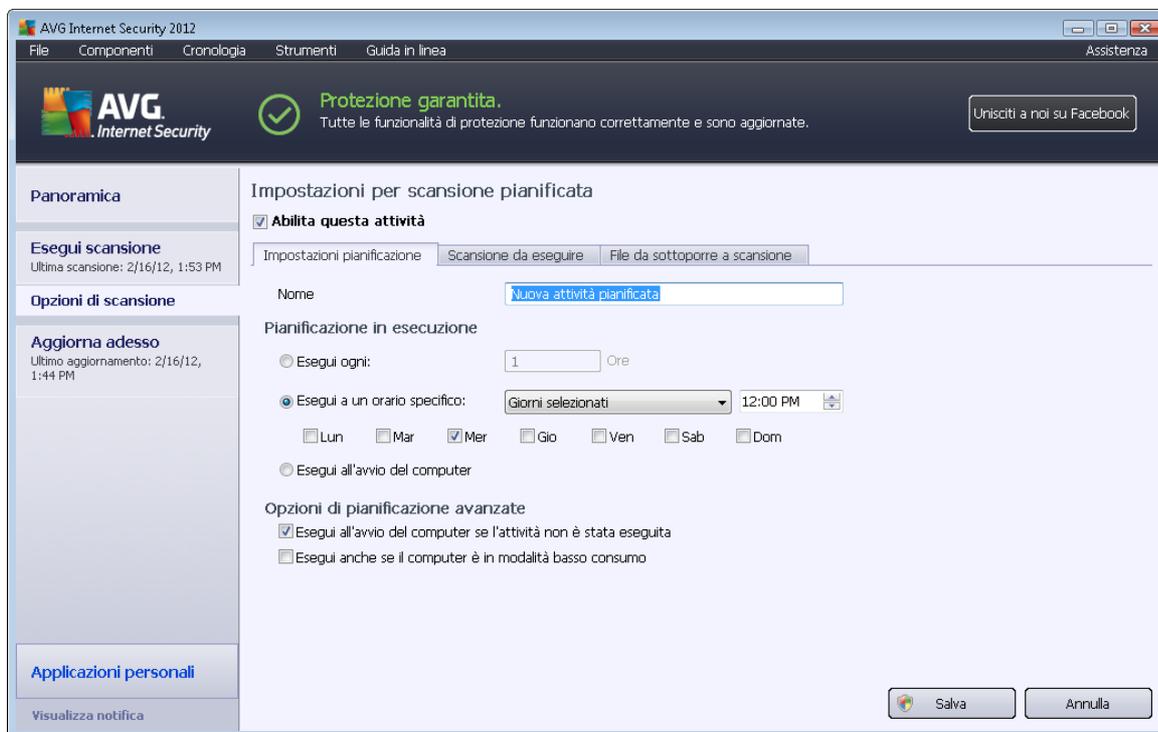
- ***Modifica pianificazione scansione***: il pulsante può essere utilizzato solo se è stato selezionato in precedenza un controllo esistente dall'elenco dei controlli pianificati. In tal caso il pulsante è visualizzato come attivo e, selezionandolo, si passa alla finestra di dialogo ***Impostazioni per scansione pianificata***, scheda Impostazioni pianificazione. I parametri del controllo selezionato sono già specificati in questa sezione e possono essere modificati.

- ***Elimina pianificazione scansione***: questo pulsante è attivo anche se è stato selezionato in precedenza un controllo esistente dall'elenco dei controlli pianificati. È possibile eliminare il controllo dall'elenco selezionando il pulsante di controllo. Tuttavia, è possibile rimuovere solo i controlli personali; non è possibile eliminare ***Pianificazione scansione intero computer*** preimpostata all'interno delle impostazioni predefinite.

- ***Indietro***: consente di tornare all'interfaccia di scansione di AVG

12.5.1. Impostazioni pianificazione

Per pianificare un nuovo controllo e il relativo avvio regolare, accedere alla finestra di dialogo ***Impostazioni per il controllo pianificato*** *(fare clic sul pulsante* ***Aggiungi pianificazione scansione*** *nella finestra di dialogo* ***Pianificazione scansioni***). La finestra di dialogo è suddivisa in tre schede: ***Impostazioni pianificazione*** *(vedere l'immagine in basso; si tratta della scheda predefinita cui si viene automaticamente reindirizzati)*, Scansione da eseguire e File da sottoporre a

scansione.

Nella scheda ***Impostazioni attività*** è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità.

Quindi, assegnare un nome alla scansione da creare e pianificare. Digitare il nome nel campo di testo dalla voce ***Nome***. Denominare le scansioni assegnando nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

Esempio: *non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via. Inoltre, non è necessario specificare nel nome della scansione se si tratta di una scansione dell'intero computer oppure relativa solo ai file o alle cartelle selezionati. Le scansioni saranno sempre una versione specifica della scansione dei file e delle cartelle selezionati.*

In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

- ***Pianificazione in esecuzione***: consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora dall'avvio ripetuto della scansione dopo un certo periodo di tempo (***Esegui ogni...***) o definendo data e ora esatte (***Esegui a un orario specifico...***) oppure definendo un evento a cui dovrà essere associato l'avvio della scansione (***Azione in base all'avvio del computer***).

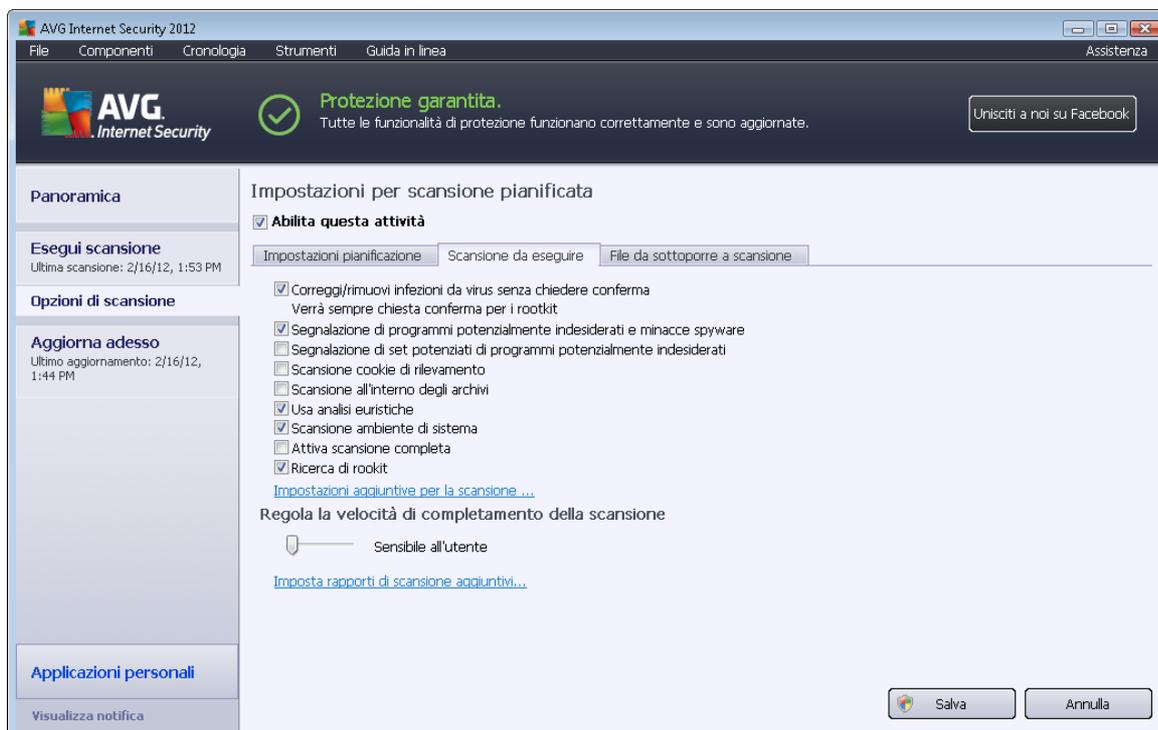
- ***Opzioni di pianificazione avanzate***: questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento.

Pulsanti di controllo delle impostazioni per la finestra di dialogo della scansione pianificata

Sono disponibili due pulsanti di controllo sulle tre schede della finestra di dialogo ***Impostazioni per scansione pianificata*** *(Impostazioni pianificazione, [Scansione da eseguire](#) e [File da sottoporre a scansione](#))*. Ciascun pulsante mantiene la stessa funzionalità indipendentemente dalla scheda visualizzata:

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla [finestra di dialogo predefinita dell'interfaccia di scansione di AVG](#). Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- ***Annulla***: consente di annullare le eventuali modifiche eseguite sulla scheda o su un'altra scheda della finestra di dialogo e di tornare alla [finestra di dialogo predefinita dell'interfaccia di scansione di AVG](#).

12.5.2. Scansione da eseguire

Nella scheda ***Scansione da eseguire*** è presente un elenco di parametri che possono essere attivati o disattivati facoltativamente. Per impostazione predefinita, la maggior parte dei parametri è attivata e la funzionalità verrà applicata durante la scansione. A meno che non esista un motivo valido per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per*

impostazione predefinita): se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente o se si decide di disattivare questa opzione, si riceverà un messaggio di notifica della presenza di un virus e si dovrà decidere l'azione da intraprendere sull'infezione rilevata. L'azione consigliata consiste nello spostare il file infetto in Quarantena virus.

  - ***Segnalazione di programmi potenzialmente indesiderati e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare il motore Anti-Spyware ed eseguire la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.
  - ***Segnalazione di set potenziati di programmi potenzialmente indesiderati*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.
  - ***Scansione cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro del componente Anti-Spyware stabilisce che i cookie devono essere rilevati durante la scansione *(i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*).
  - ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.
  - ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
  - ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.
  - ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rookit*** (*attivata per impostazione predefinita*): la scansione Anti-Rootkit cerca nel computer possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Quindi, è possibile modificare la configurazione della scansione come segue:

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:

  - ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

  - ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

    - ***Tutti i tipi di file*** con la possibilità di definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione;

    - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus.*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

    - Facoltativamente, è possibile sottoporre a scansione i file senza estensione tramite ***Effettuare la scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificare questa impostazione a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente per l'utilizzo automatico delle risorse.* In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer ma la durata della scansione non influisce*) o più velocemente con utilizzo delle risorse di sistema più elevato (*ad esempio quando l'utente è temporaneamente lontano dal computer*).

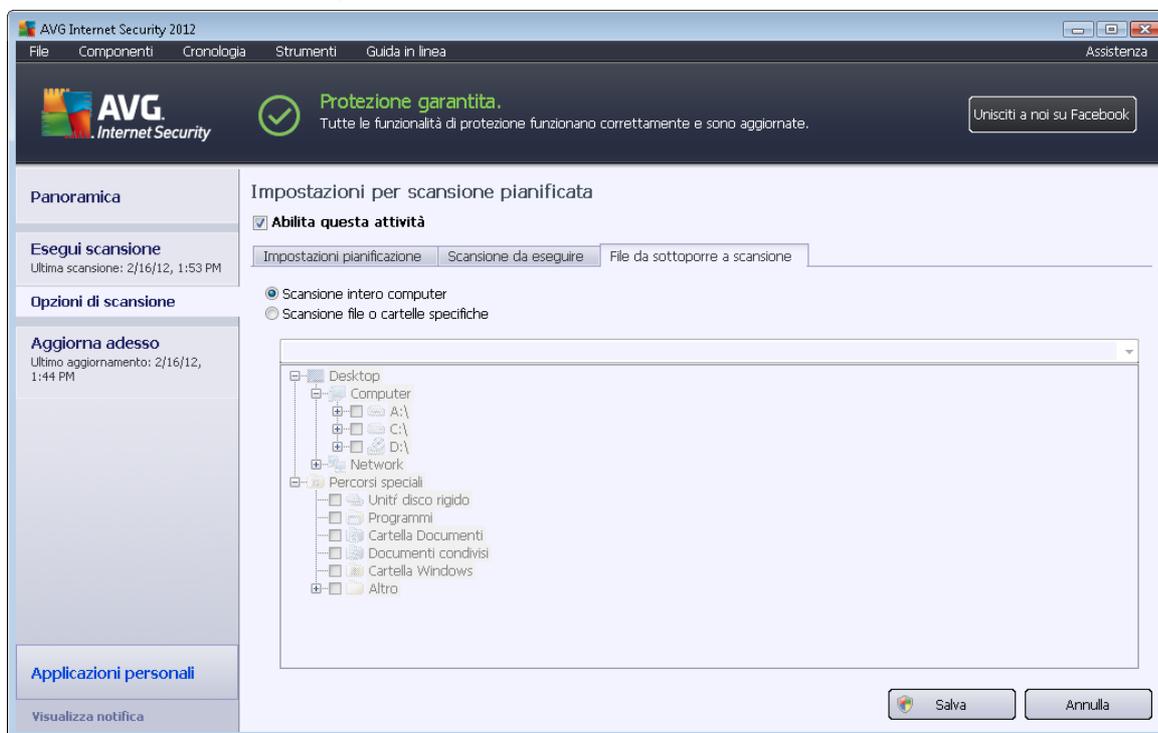
- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare:

Pulsanti di controllo

Sono disponibili due pulsanti di controllo sulle tre schede della finestra di dialogo ***Impostazioni per scansione pianificata*** (*Impostazioni pianificazione, Scansione da eseguire e File da sottoporre a scansione*) e tutti hanno la stessa funzionalità indipendentemente dalla scheda visualizzata:

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- ***Annulla***: consente di annullare le eventuali modifiche eseguite sulla scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG.

12.5.3. File da sottoporre a scansione

Nella scheda ***File da sottoporre a scansione*** è possibile definire se si desidera pianificare la [scansione dell'intero computer](#) o la [scansione di file o cartelle specifiche](#).

Se si seleziona la scansione di cartelle o file specifici, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione (*espandere le voci facendo clic sul nodo "+" finché non viene individuata la cartella da sottoporre a scansione*). È possibile selezionare più cartelle facendo clic sulle rispettive caselle. Le cartelle selezionate verranno visualizzate nel campo di testo nella parte superiore della finestra di dialogo e nel menu a discesa verrà mantenuta la cronologia delle scansioni selezionate per riferimento futuro. In alternativa, è possibile immettere manualmente il percorso completo della cartella desiderata (*se si immettono più percorsi, è necessario separarli con un punto e virgola senza ulteriori spazi*).

All'interno della struttura è inoltre possibile visualizzare un ramo denominato ***Percorsi speciali***. Di seguito è disponibile un elenco delle posizioni che verranno sottoposte a scansione se verrà selezionata la relativa casella di controllo:

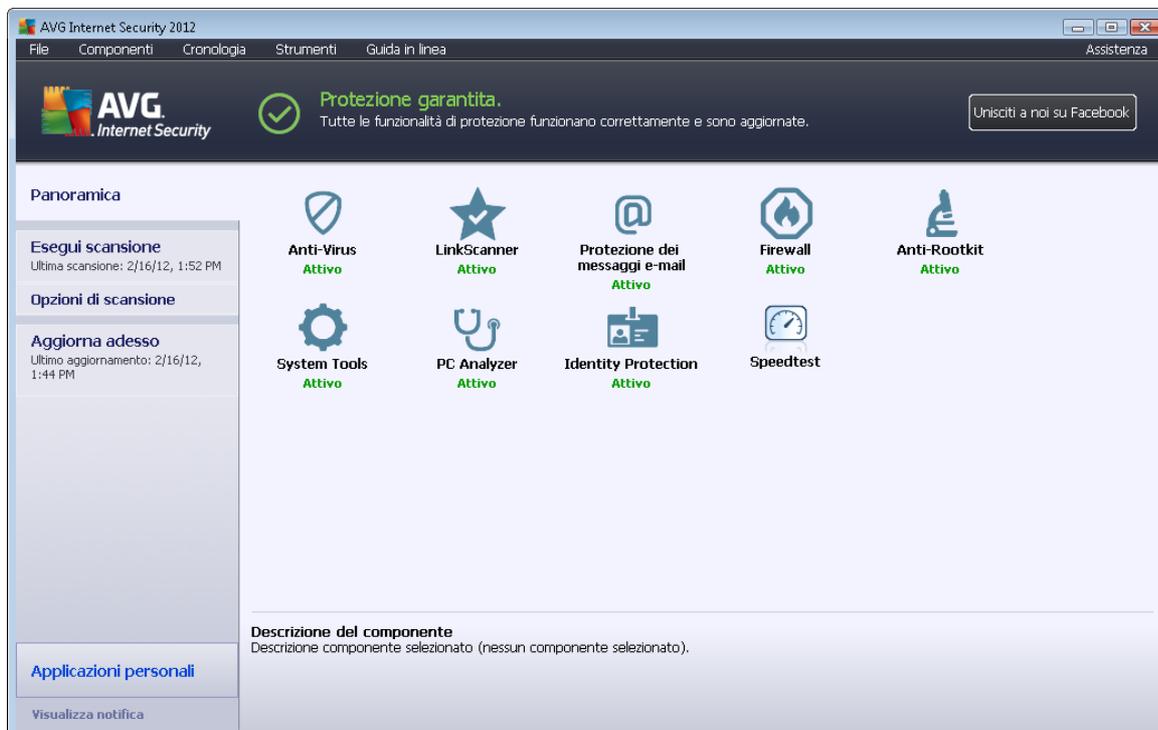
- ***Dischi rigidi locali***: tutti i dischi rigidi del computer
- ***Programmi***
  - C:\Programmi\
  - *nella versione a 64 bit* C:\Programmi (x86)

- ***Cartella Documenti***
  - *per Windows XP:* C:\Documents and Settings\utente predefinito\Documenti\
  - *per Windows Vista/7*: C:\Users\utente\Documenti\
- ***Documenti condivisi***
  - *per Windows XP*: C:\Documents and Settings\All Users\Documenti condivisi\
  - *per Windows Vista/7*: C:\Users\Public\Documenti condivisi\
- ***Cartella Windows***: C:\Windows\
- ***Altro***
  - *Unità di sistema*: disco rigido su cui è installato il sistema operativo (solitamente C:)
  - *Cartella di sistema*: C:\Windows\System32\
  - *Cartella file temporanei*: C:\Documents and Settings\utente\Local\ (*Windows XP*) oppure C:\Users\utente\AppData\Local\Temp\ (*Windows Vista/7*)
  - *File temporanei di Internet*: C:\Documents and Settings\utente\Local Settings\Temporary Internet Files\ (*Windows XP*); oppure C:\Users\utente\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Pulsanti di controllo

Gli stessi due pulsanti di controllo sono disponibili nelle tre schede della finestra di dialogo ***Impostazioni per scansione pianificata*** *(Impostazioni pianificazione, Scansione da eseguire e File da sottoporre a scansione)*:

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.
- ***Annulla***: consente di annullare le eventuali modifiche eseguite sulla scheda o su un'altra scheda della finestra di dialogo e di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG.

12.6. Panoramica di Risultati scansione

La finestra di dialogo ***Panoramica risultati di scansione*** è accessibile dall'interfaccia di scansione di AVG tramite il pulsante ***Cronologia scansione***. Nella finestra di dialogo è contenuto l'elenco di tutte le scansioni avviate in precedenza e le informazoni dei risultati relativi:

- ***Nome***: nome della scansione; può essere il nome di una delle scansioni predefinite o il nome assegnato alla propria scansione pianificata. Ciascun nome include un'icona che indica i risultati della scansione:

  – il colore verde indica che non è stata rilevata alcuna infezione durante la scansione

  – il colore blu indica che è stata rilevata un'infezione durante la scansione ma l'oggetto infetto è stato rimosso automaticamente

  – il colore rosso indica che è stata rilevata un'infezione durante la scansione ma non è stato possibile rimuoverla.

  Ciascuna icona può essere intera o suddivisa in due parti: l'icona intera indica una scansione completata correttamente, l'icona suddivisa in due indica una scansione annullata o interrotta.

  Nota*: per informazioni dettagliate su ciascuna icona vedere la finestra di dialogo Risultati scansione accessibile tramite il pulsante Visualizza dettagli (nella parte inferiore della finestra di dialogo).*

- ***Ora di inizio***: data e ora di avvio della scansione
- ***Ora di fine***: data e ora del completamento della scansione
- ***Oggetti controllati***: numero di oggetti controllati durante la scansione
- ***Infezioni***: numero delle infezioni da virus rilevate / rimosse
- ***Spyware*** : numero di spyware rilevato / rimosso
- ***Avvisi***: numero di oggetti sospetti
- ***Rootkit***: numero di rootkit
- ***Informazioni registro di scansione***: informazioni relative all'andamento e al risultato della scansione (in genere in relazione alla finalizazzione o all'interruzione)

Pulsanti di controllo

I pulsanti di controllo per la finestra di dialogo ***Panoramica risultati di scansione*** sono i seguenti:

- ***Visualizza dettagli***: selezionare questa opzione per accedere alla finestra di dialogo Risultati scansione e visualizzare dati dettagliati relativi alla scansione selezionata
- ***Elimina risultato***: selezionare questa opzione per rimuovere la voce selezionata dalla panoramica dei risultati di scansione
- ***Indietro***: consente di tornare alla finestra di dialogo predefinita dell'interfaccia di scansione di AVG

12.7. Dettagli di Risultati scansione

Se nella finestra di dialogo Panoramica risultati di scansione è selezionata una scansione specifica, è possibile fare clic sul pulsante ***Visualizza dettagli*** per passare alla finestra di dialogo ***Risultati scansione*** che contiene i dati dettagliati sul corso e sui risultati della scansione selezionata. La finestra di dialogo è suddivisa in altre schede:

- Panoramica dei risultati: questa scheda viene sempre visualizzata e fornisce i dati statistici che descrivono l'avanzamento della scansione
- Infezioni: questa scheda viene visualizzata solo se durante la scansione è stata rilevata un'infezione da virus
- Spyware: questa scheda viene visualizzata solo se durante la scansione è stato rilevato spyware
- Avvisi: questa scheda viene visualizzata, ad esempio, se sono stati rilevati cookie durante la scansione
- Rootkit: questa scheda viene visualizzata solo se durante la scansione sono stati rilevati

rootkit

- [Informazioni](): questa scheda viene visualizzata solo se sono state rilevate alcune potenziali minacce non classificabili in nessuna delle categorie suddette; nella scheda viene visualizzato un messaggio di avviso sul rilevamento. Inoltre, qui sono disponibili informazioni sugli oggetti che non è stato possibile sottoporre a scansione *(ad esempio archivi protetti da password)*.

12.7.1. Scheda Panoramica dei risultati

Nella scheda ***Risultati scansione*** sono contenuti i dettagli delle statistiche con informazioni in relazione a:

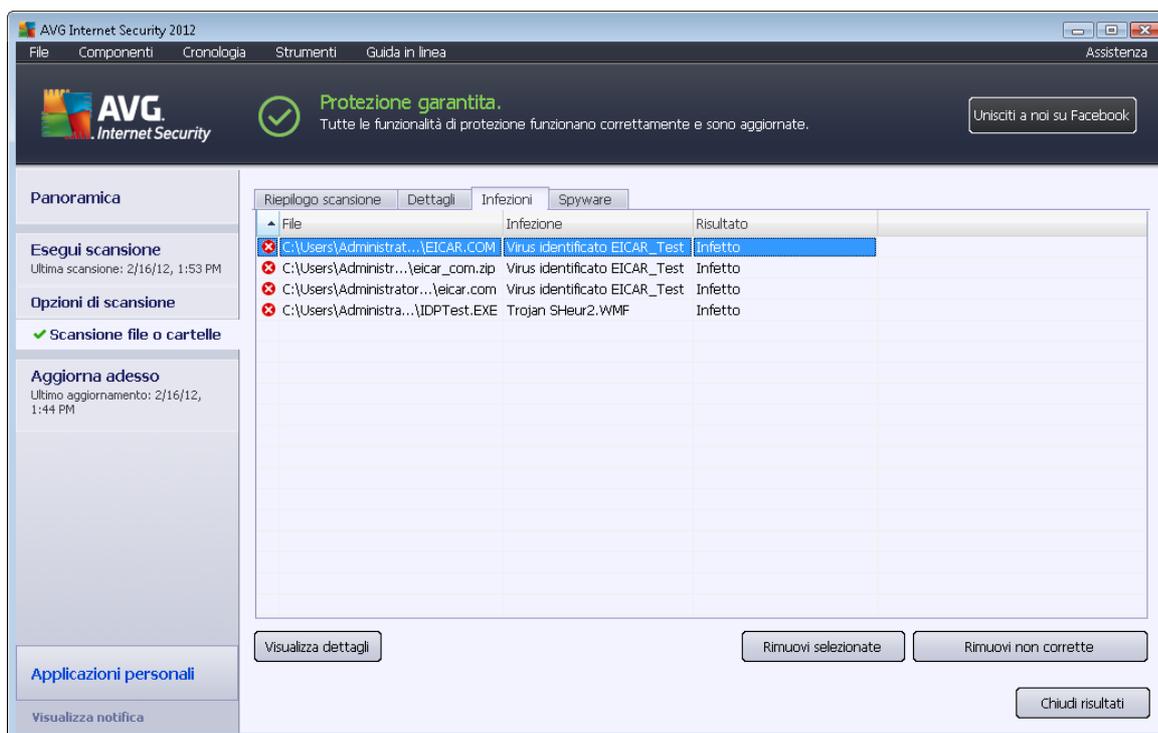
- infezioni da virus / spyware rilevate
- infezioni da virus / spyware rimosse
- numero di infezioni da virus / spyware che non è possibile rimuovere o correggere

Inoltre, sono contenute informazioni sulla data e sull'ora esatte di avvio della scansione, sul numero totale di oggetti sottoposti a scansione, sulla durata della scansione e sul numero di errori che si sono verificati durante la scansione.

Pulsanti di controllo

In questa finestra di dialogo è disponibile solo un pulsante di controllo. Il pulsante ***Chiudi risultati***

consente di tornare alla finestra di dialogo Panoramica risultati di scansione.

12.7.2. Scheda Infezioni

La scheda ***Infezioni*** viene visualizzata nella finestra di dialogo ***Risultati scansione*** solo se è stata rilevata un'infezione da virus durante la scansione. La scheda è suddivisa in tre sezioni in cui sono contenute le seguenti informazioni:

- ***File***: percorso completo della posizione originale dell'oggetto infetto
- ***Infezioni***: nome del virus rilevato (*per informazioni dettagliate su virus specifici, consultare l'Enciclopedia dei virus in linea*)
- ***Risultato***: definisce lo stato corrente dell'oggetto infetto rilevato durante la scansione:
  - ***Infetto***: l'oggetto infetto è stato rilevato e lasciato nella sua posizione originale (*ad esempio, se è stata disattivata l'opzione di correzione automatica nelle impostazioni di una scansione specifica*)
  - ***Corretto***: l'oggetto infetto è stato corretto automaticamente e lasciato nella sua posizione originale
  - ***Spostato in Quarantena virus***: l'oggetto infetto è stato spostato in Quarantena virus
  - ***Eliminato***: l'oggetto infetto è stato eliminato
  - ***Aggiunto alle eccezioni PUP***: l'oggetto rilevato è stato classificato come

eccezione ed è stato aggiunto all'elenco delle eccezioni PUP *(configurato nella finestra di dialogo [Eccezioni PUP]() delle impostazioni avanzate)*

- ***File bloccato: non verificato*** - l'oggetto corrispondente è bloccato pertanto AVG non è in grado di sottoporlo a scansione
- ***Oggetto potenzialmente pericoloso***: l'oggetto è stato rilevato come potenzialmente pericoloso ma non infetto (*potrebbe contenere macro, ad esempio*); l'informazione deve essere considerata solo come un avviso
- ***È necessario riavviare il computer per concludere l'operazione***: non è possibile rimuovere l'oggetto infetto. Per rimuoverlo definitivamente, è necessario riavviare il computer

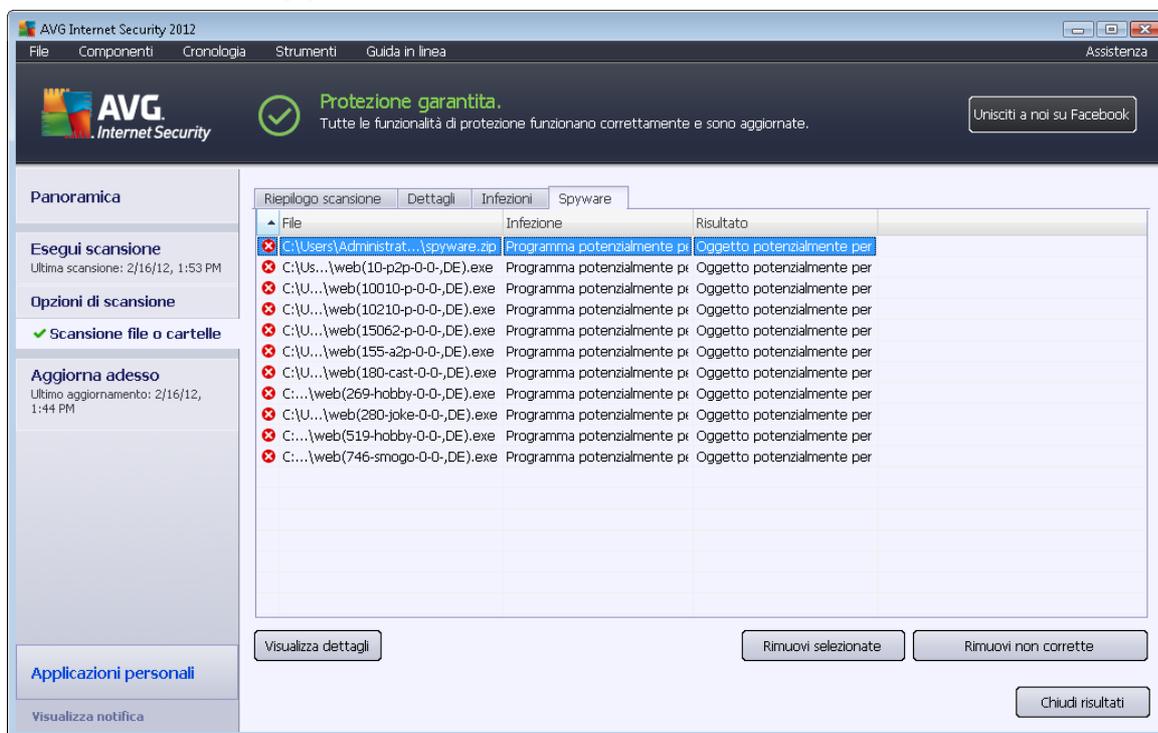
Pulsanti di controllo

Sono disponibili tre pulsanti di controllo in questa finestra di dialogo:

- ***Visualizza dettagli***: il pulsante consente di aprire una nuova finestra di dialogo relativa alle ***informazioni dettagliate sull'oggetto***:

In questa finestra di dialogo sono disponibili informazioni dettagliate sull'oggetto infetto rilevato (*ad esempio nome e posizione dell'oggetto infetto, tipo di oggetto, tipo di SDK, risultato del rilevamento e cronologia delle azioni correlate all'oggetto rilevato*). I pulsanti ***Indietro*** / ***Avanti*** consentono di visualizzare informazioni su rilevamenti specifici. Utilizzare il pulsante ***Chiudi*** per chiudere questa finestra di dialogo.

- ***Rimuovi selezionate***: utilizzare il pulsante per spostare l'oggetto rilevato selezionato in [Quarantena virus]()
- ***Rimuovi non corrette***: questo pulsante consente di eliminare tutti gli oggetti rilevati che non possono essere corretti né spostati in [Quarantena virus]()
- ***Chiudi risultati***: consente di uscire dalla panoramica delle informazioni dettagliate e di tornare alla finestra di dialogo [Panoramica risultati di scansione]()

12.7.3. Scheda Spyware

La scheda ***Spyware*** viene visualizzata nella finestra di dialogo ***Risultati scansione*** solo se durante la scansione sono stati rilevati spyware. La scheda è suddivisa in tre sezioni in cui sono contenute le seguenti informazioni:

- ***File***: percorso completo della posizione originale dell'oggetto infetto
- ***Infezioni***: nome dello spyware rilevato (*per informazioni dettagliate su virus specifici, consultare l'Enciclopedia dei virus in linea)*
- ***Risultato***: definisce lo stato corrente dell'oggetto rilevato durante la scansione:
    - ***Infetto***: l'oggetto infetto è stato rilevato e lasciato nella sua posizione originale *(ad esempio, se è stata disattivata l'opzione di correzione automatica nelle impostazioni di una scansione specifica)*
    - ***Corretto***: l'oggetto infetto è stato corretto automaticamente e lasciato nella sua posizione originale
    - ***Spostato in Quarantena virus***: l'oggetto infetto è stato spostato in Quarantena virus
    - ***Eliminato***: l'oggetto infetto è stato eliminato
    - ***Aggiunto alle eccezioni PUP***: l'oggetto rilevato è stato classificato come eccezione ed è stato aggiunto all'elenco delle eccezioni PUP *(configurato nella finestra di dialogo Eccezioni PUP delle impostazioni avanzate)*

- *File bloccato: non verificato*: l'oggetto corrispondente è stato bloccato pertanto AVG non è in grado di sottoporlo a scansione
- ***Oggetto potenzialmente pericoloso***: l'oggetto è stato rilevato come potenzialmente pericoloso ma non infetto (potrebbe contenere macro, ad esempio); l'informazione deve essere considerata solo come un avviso
- ***È necessario riavviare il computer per concludere l'operazione***: non è possibile rimuovere l'oggetto infetto. Per rimuoverlo definitivamente, è necessario riavviare il computer

Pulsanti di controllo

Sono disponibili tre pulsanti di controllo in questa finestra di dialogo:

- ***Visualizza dettagli***: il pulsante consente di aprire una nuova finestra di dialogo relativa alle ***informazioni dettagliate sull'oggetto***:

  In questa finestra di dialogo sono disponibili informazioni dettagliate sull'oggetto infetto rilevato (*ad esempio nome e posizione dell'oggetto infetto, tipo di oggetto, tipo di SDK, risultato del rilevamento e cronologia delle azioni correlate all'oggetto rilevato*). I pulsanti ***Indietro*** / ***Avanti*** consentono di visualizzare informazioni su rilevamenti specifici. Utilizzare il pulsante ***Chiudi*** per uscire da questa finestra di dialogo.

- ***Rimuovi selezionate***: utilizzare il pulsante per spostare l'oggetto rilevato selezionato in Quarantena virus
- ***Rimuovi non corrette***: questo pulsante consente di eliminare tutti gli oggetti rilevati che non possono essere corretti né spostati in Quarantena virus
- ***Chiudi risultati***: consente di uscire dalla panoramica delle informazioni dettagliate e di tornare alla finestra di dialogo Panoramica risultati di scansione

12.7.4. Scheda Avvisi

La scheda ***Avvisi*** consente di visualizzare le informazioni relative agli oggetti "sospetti" (*file, generalmente*) rilevati durante la scansione. Quando vengono rilevati da Resident Shield, l'accesso a questi file viene bloccato. Esempi tipici di questo tipo di rilevamenti sono: file nascosti, cookie, chiavi del Registro di sistema sospette, archivi o documenti protetti da password e così via. Tali file non presentano minacce dirette per il computer o la sicurezza. Le informazioni su questi file sono generalmente utili in caso venga individuato adware o spyware sul computer. Se nei risultati del controllo sono presenti solo Avvisi rilevati da **AVG Internet Security 2012**, non è necessaria alcuna azione.

Questa è una breve descrizione degli esempio più comuni di tali oggetti:

- ***File nascosti***: i file nascosti, per impostazione predefinita, non sono visibili in Windows e alcuni virus o altre minacce potrebbero tentare di evitare il rilevamento memorizzando i propri file con questo attributo. Se **AVG Internet Security 2012** segnala un file nascosto che si ritiene dannoso, è possibile spostarlo in Quarantena virus.

- ***Cookie***: i cookie sono file di testo che vengono utilizzati dai siti Web per memorizzare informazioni specifiche dell'utente, che vengono in seguito utilizzate per caricare layout personalizzati del sito Web, pre-immettere il nome utente e così via.

- ***Chiavi del Registro di sistema sospette***: alcuni tipi di malware memorizzano le proprie informazioni nel Registro di sistema di Windows per garantire che vengano caricate all'avvio del computer o per estenderne gli effetti al sistema operativo.

12.7.5. Scheda Rootkit

La scheda ***Rootkit*** visualizza le informazioni sui rootkit rilevati durante la scansione anti-rootkit inclusa nella Scansione intero computer.

Un rootkit è un programma progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. L'accesso all'hardware è raramente necessario poiché un rootkit dovrà assumere il controllo del sistema operativo in esecuzione sull'hardware. In genere, i rootkit agiscono per nascondere la propria presenza sul sistema tramite sovversione o espedienti relativi ai meccanismi di protezione standard del sistema operativo. Si tratta spesso anche di trojan che ingannano gli utenti facendo loro credere di poter essere eseguiti in tutta sicurezza sui sistemi. Le tecniche utilizzate a questo scopo possono includere l'occultamento di processi in esecuzione dai programmi di monitoraggio oppure di file o dati di sistema dal sistema operativo.

La struttura di questa scheda corrisponde sostanzialmente a quella della scheda Infezioni o della scheda Spyware.

12.7.6. Scheda Informazioni

Nella scheda ***Informazioni*** sono contenuti i dati sui rilevamenti che non possono essere classificati come infezioni, spyware e così via. Non possono essere etichettati come pericolosi anche se devono essere considerati attentamente. La scansione **AVG Internet Security 2012** è in grado di rilevare i file sospetti benché non infetti. Questo tipo di file viene segnalato come Avviso oppure Informazioni.

Le ***Informazioni*** sul livello di gravità possono essere segnalate per uno dei motivi seguenti:

- ***Run-time compresso***: il file è stato compresso con uno dei compressori run-time meno comuni. Questa situazione può indicare un tentativo di impedire la scansione del file. Non tutte le segnalazioni di file di questo tipo indicano tuttavia la presenza di un virus.

- ***Run-time compresso ricorsivo***: la situazione è simile a quella descritta sopra, ma meno frequente tra i programmi software di uso comune. Questo tipo di file è sospetto ed è consigliabile rimuoverlo o inviarlo per l'analisi.

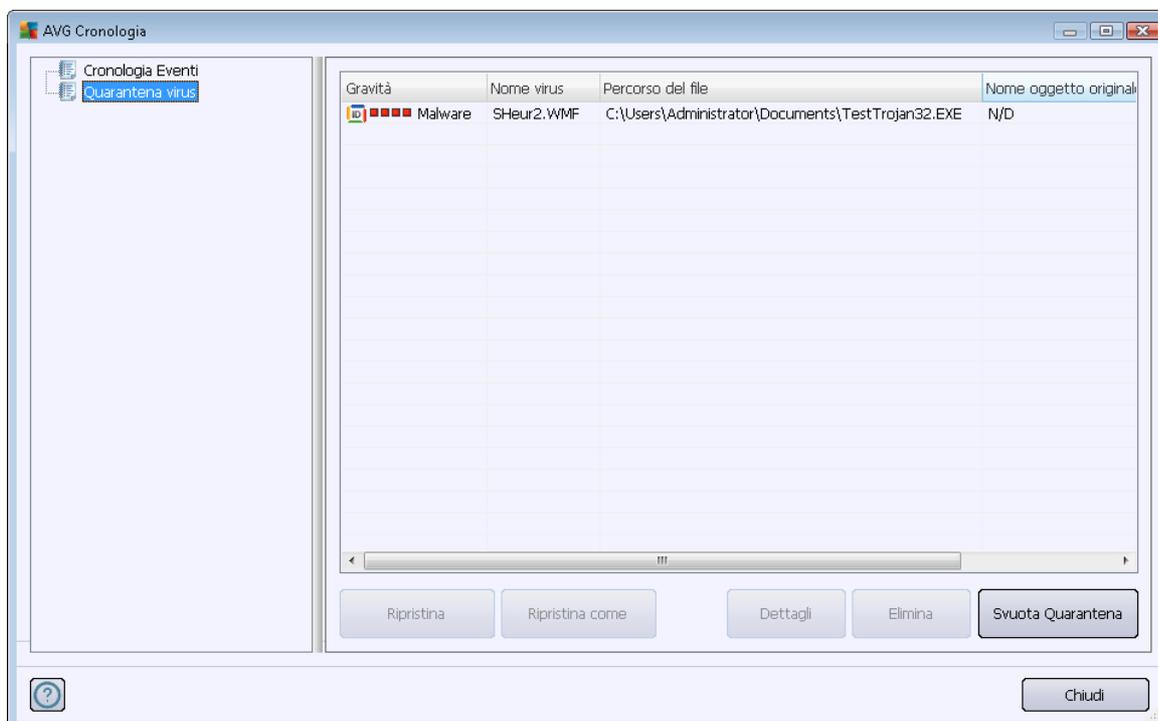
- ***Archivio o documento protetto da password***: i file protetti da password non possono essere sottoposti a scansione da **AVG Internet Security 2012** (*o da altri programmi anti-malware*).

- ***Documenti con macro***: il documento segnalato contiene macro che possono essere dannose.

- ***Estensione nascosta***: i file con estensioni nascoste potrebbero sembrare, ad esempio, immagini, ma in realtà sono file eseguibili (*ad esempio immagine.jpg.exe*). La seconda estensione non è visibile in Windows per impostazione predefinita e **AVG Internet Security 2012** segnala tali file per impedirne l'apertura accidentale.

- ***Percorso di file non appropriato***: se un file di sistema importante viene eseguito da un percorso diverso da quello predefinito (*ad esempio winlogon.exe eseguito da una cartella diversa da Windows*), **AVG Internet Security 2012** segnala questa discrepanza. In alcuni casi, i virus utilizzano nomi di processi di sistema standard per rendere meno visibile la propria presenza nel sistema.

- ***File bloccato***: il file segnalato è bloccato, pertanto non può essere sottoposto a scansione da **AVG Internet Security 2012**. Ciò significa solitamente che il file viene costantemente utilizzato dal sistema (*ad esempio un file di scambio*).

12.8. Quarantena virus

Quarantena virus è un ambiente protetto per la gestione degli oggetti sospetti o infetti rilevati durante i controlli AVG. Se durante la scansione viene rilevato un oggetto infetto e AVG non è in grado di ripararlo automaticamente, viene richiesto quale operazione eseguire sull'oggetto sospetto. La soluzione consigliata è spostare l'oggetto in ***Quarantena virus*** per un'ulteriore elaborazione. Lo scopo principale di ***Quarantena virus*** è quello di conservare ciascun file eliminato per un periodo di tempo sufficiente ad accertare che il file non sia più necessario nella posizione originale. Se l'assenza del file dovesse causare problemi, è possibile inviare il file in questione per l'analisi o ripristinarlo nella posizione originale.

L'interfaccia di ***Quarantena virus*** viene aperta in una finestra separata e offre una panoramica delle informazioni relative agli oggetti infetti messi in quarantena:

- ***Gravità***: se è stato installato il componente Identity Protection in **AVG Internet Security 2012**, questa sezione fornirà l'identificazione grafica della gravità del rilevamento in base a una scala a quattro livelli dal più sicuro (■□□□) al più pericoloso (■■■■) e informazioni sul tipo di infezione (*in base al livello di infezione; tutti gli oggetti elencati possono essere sicuramente o potenzialmente infetti*)

- ***Nome virus***: specifica il nome dell'infezione rilevata in base all'Enciclopedia dei virus *(in linea)*

- ***Percorso del file***: percorso completo della posizione originale del file infetto rilevato

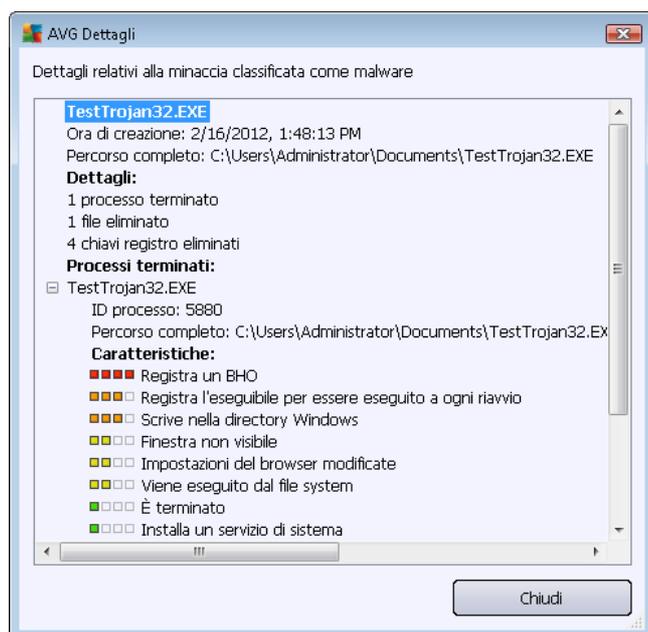
- ***Nome oggetto originale***: tutti gli oggetti rilevati inseriti nell'elenco sono stati denominati con un nome standard assegnato da AVG durante il processo di scansione. Se un oggetto

aveva uno specifico nome originale conosciuto dal sistema (*ad esempio il nome di un allegato e-mail che non corrisponde al contenuto effettivo dell'allegato*), tale nome verrà visualizzato in questa colonna.

- ***Data di archiviazione***: data e ora del rilevamento e dell'inserimento in Quarantena virus

Pulsanti di controllo

I seguenti pulsanti di controllo sono accessibili dall'interfaccia di ***Quarantena virus***:

- ***Ripristina***: consente di ripristinare il file infetto nella posizione originale sul disco
- ***Ripristina come***: sposta il file infetto nella cartella selezionata
- ***Dettagli***: questo pulsante è applicabile alle sole minacce rilevate da Identity Protection. Una volta selezionato, visualizza una panoramica sinottica dei dettagli della minaccia (*file/ processi interessati, caratteristiche del processo e così via*). Tenere presente che per tutti gli elementi non rilevati da IDP questo pulsante è ombreggiato e non attivo.

- ***Elimina***: consente di rimuovere definitivamente il file infetto da ***Quarantena virus***
- ***Svuota Quarantena***: elimina completamente tutto il contenuto di ***Quarantena Virus***. I file rimossi da ***Quarantena virus*** vengono eliminati in modo definitivo dal disco (*non vengono spostati nel Cestino*).

13. Aggiornamenti di AVG

Nessun software di protezione è in grado di garantire una vera protezione dai vari tipi di minacce se non viene aggiornato con regolarità. Gli autori dei virus ricercano di continuo nuove imperfezioni da sfruttare sia nei sistemi operativi che nel software. Tutti i giorni si presentano nuovi virus, nuovi malware e nuovi attacchi di hacker. Per questa ragione, i fornitori di software rilasciano regolarmente aggiornamenti e patch di protezione per correggere eventuali difetti della protezione che vengono rilevati.

Considerando le nuove minacce informatiche emergenti, e la velocità con cui si diffondono, è assolutamente fondamentale aggiornare **AVG Internet Security 2012** regolarmente. La soluzione migliore è rappresentata dall'attenersi alle impostazioni predefinite del programma in cui è stato configurato l'aggiornamento automatico. Tenere presente che, se il database dei virus di **AVG Internet Security 2012** non è aggiornato, il programma non sarà in grado di rilevare le minacce più recenti.

È fondamentale aggiornare AVG con regolarità. Gli aggiornamenti delle definizione dei virus principali dovrebbero essere eseguiti ogni giorno, se possibile. Gli aggiornamenti del programma meno urgenti possono essere eseguiti settimanalmente.

13.1. Avvio degli aggiornamenti

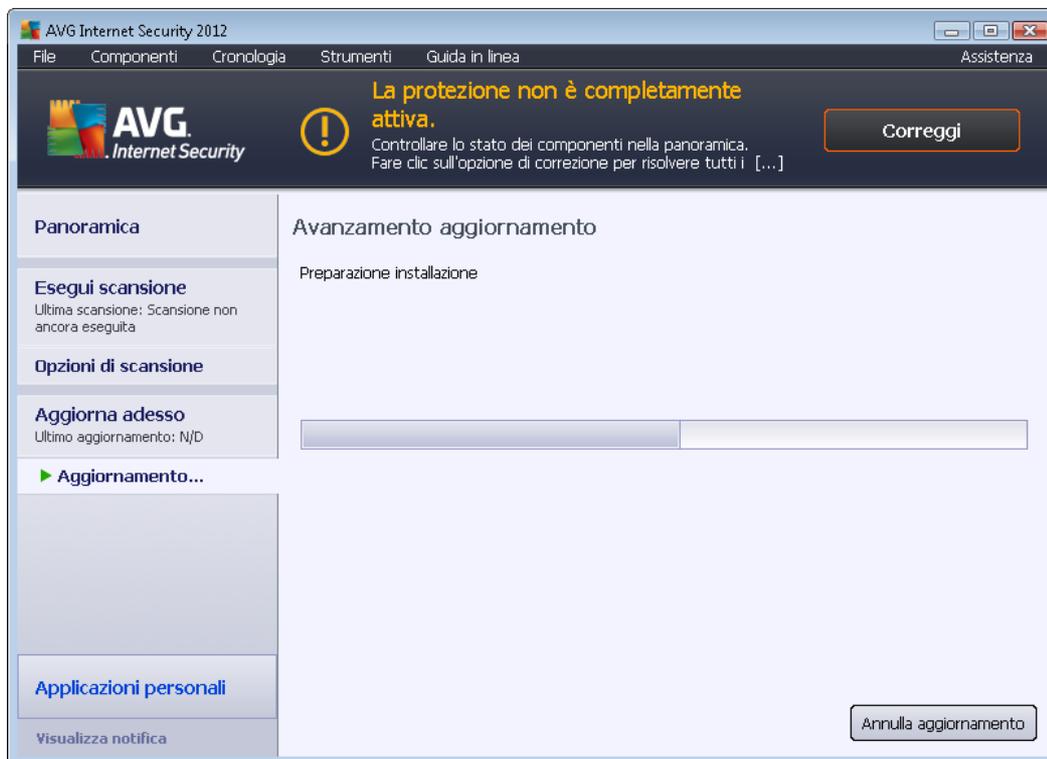
Per fornire la protezione massima, **AVG Internet Security 2012** per impostazione predefinita ricerca nuovi aggiornamenti ogni quattro ore. Poiché gli aggiornamenti AVG non vengono rilasciati in base a una pianificazione fissa, ma in base alla quantità e alla gravità di nuove minacce, questo check-up è molto importante per assicurare che il database dei virus di AVG sia sempre aggiornato.

Se si desiderasse ridurre il numero di aggiornamenti avviati, è possibile impostare parametri di avvio degli aggiornamenti personalizzati. Tuttavia, si consiglia di avviare l'aggiornamento almeno una volta al giorno. La configurazione può essere modificata nella sezione Impostazioni avanzate/ Pianificazioni, in particolare nelle seguenti finestre di dialogo:

- Pianificazione aggiornamento definizioni
- Pianificazione aggiornamento del programma
- Pianificazione aggiornamenti Anti-Spam

Per controllare la presenza di nuovi file di aggiornamento immediatamente, utilizzare il collegamento rapido Aggiorna adesso nell'interfaccia utente principale. Questo collegamento è sempre disponibile da qualsiasi finestra di dialogo dell'interfaccia utente.

13.2. Avanzamento dell'aggiornamento

Una volta avviato l'aggiornamento, AVG verificherà innanzitutto se sono presenti nuovi file di aggiornamento. In caso affermativo, **AVG Internet Security 2012** ne effettuerà il download e avvierà il processo di aggiornamento. Durante il processo di aggiornamento si verrà reindirizzati all'interfaccia di ***Aggiornamento***, da cui è possibile visualizzare la rappresentazione grafica e la panoramica dei parametri statistici rilevanti dell'avanzamento del processo *(dimensione dei file di aggiornamento, dati ricevuti, velocità di download, tempo trascorso e così via)*:

***Nota**: prima dell'avvio di un aggiornamento di AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare il sistema operativo nella configurazione originale da questo punto. Questa opzione è accessibile tramite Start / Tutti i programmi / Accessori / Utilità di sistema / Ripristino configurazione di sistema. L'operazione è consigliata ai soli utenti esperti.*

13.3. Livelli di aggiornamento

AVG Internet Security 2012 offre due livelli di aggiornamento selezionabili:

- ***In Aggiornamento definizioni*** sono contenute le modifiche necessarie per una protezione anti-virus, anti-spam e anti-malware affidabile. In genere, non include eventuali modifiche del codice e consente di aggiornare solo il database delle definizioni. Questo aggiornamento deve essere applicato non appena si rende disponibile.

- ***In Aggiornamento programma*** sono contenuti le modifiche, le correzioni e i miglioramenti del programma.

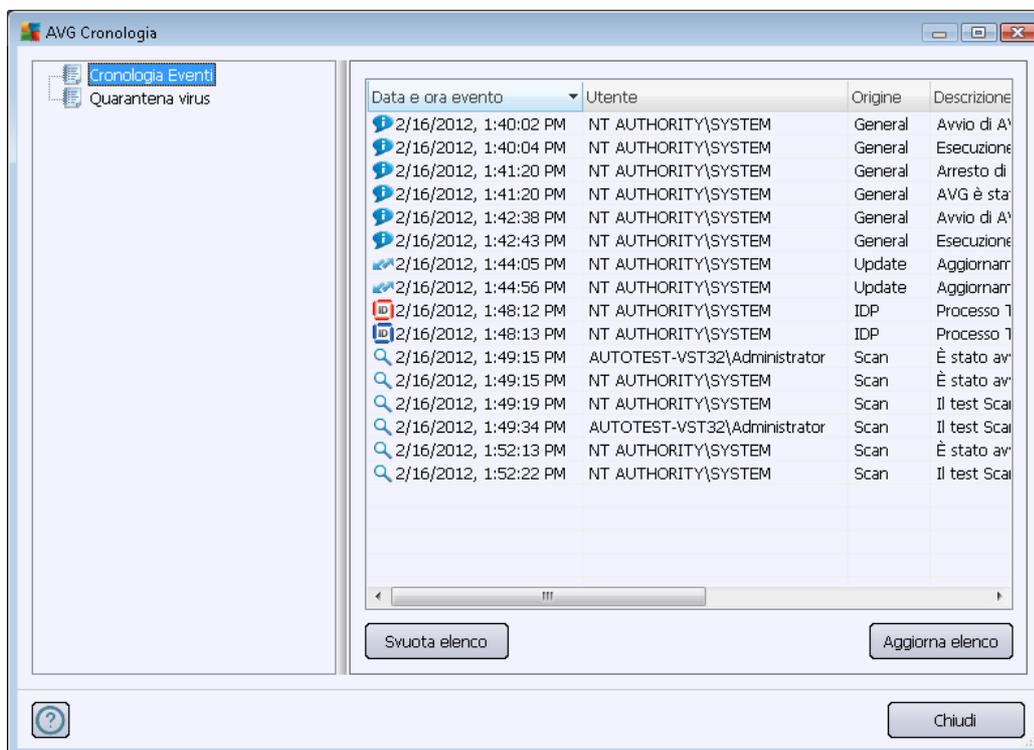
Nel corso della pianificazione di un aggiornamento, è possibile definire parametri specifici per entrambi i livelli di aggiornamento:

- Pianificazione aggiornamento definizioni

- Pianificazione aggiornamento del programma

***Nota:** se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata*

dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta.

14. Cronologia eventi

La finestra di dialogo ***Cronologia*** è accessibile dal menu di sistema tramite la voce ***Cronologia/ Log della Cronologia Eventi***. In questa finestra di dialogo è possibile trovare un riepilogo di importanti eventi che si sono verificati durante l'attività di **AVG Internet Security 2012**. Nella ***Cronologia*** vengono registrati i seguenti tipi di evento:

- Informazioni sugli aggiornamenti dell'applicazione AVG
- Informazioni su inizio, fine o arresto della scansione (*inclusi i controlli eseguiti automaticamente*)
- Informazioni sugli eventi connessi al rilevamento di virus (*da parte di Resident Shield o della scansione*) inclusa la relativa posizione
- Altri eventi importanti

Per ciascun evento vengono indicate le seguenti informazioni:

- ***Data e ora evento*** indica la data e l'ora esatte in cui si è verificato l'evento
- ***Utente*** indica il nome dell'utente connesso nel momento in cui si è verificato l'evento
- ***Origine*** fornisce informazioni sul componente di origine o altra parte del sistema AVG che ha attivato l'evento
- ***Descrizione evento*** offre un breve riepilogo dell'evento che si è verificato

Pulsanti di controllo

- ***Svuota elenco***: fare clic su questo pulsante per eliminare tutte le voci incluse nell'elenco degli eventi
- ***Aggiorna elenco***: fare clic su questo pulsante per aggiornare tutte le voci incluse nell'elenco degli eventi

15. Domande frequenti e assistenza tecnica

Se si verificano problemi di tipo commerciale o tecnico con l'applicazione **AVG Internet Security 2012**, sono disponibili diversi modi per richiedere assistenza. Effettuare la scelta tra le seguenti opzioni:

- ***Ottieni assistenza***: direttamente dall'applicazione AVG è possibile visualizzare una pagina dedicata dell'assistenza clienti sul sito Web di AVG (http://www.avg.com/). Selezionare la voce del menu principale ***Guida / Ottieni assistenza*** per essere reindirizzati a una pagina del sito Web di AVG con le opzioni di assistenza disponibili. Per procedere, seguire le istruzioni fornite nella pagina Web.

- ***Assistenza (collegamento nel menu principale)***: il menu dell'applicazione AVG (*nella parte superiore dell'interfaccia utente principale*) include il collegamento ***Assistenza*** che apre una nuova finestra di dialogo contenente tutti i tipi di informazioni necessarie per ricevere assistenza. La finestra di dialogo include dati di base sul programma AVG installato (*versione programma/database*), dettagli della licenza e un elenco di collegamenti rapidi per l'assistenza:

- ***Risoluzione dei problemi nella Guida***: una nuova sezione ***Risoluzione dei problemi*** è disponibile direttamente nel file della Guida incluso in **AVG Internet Security 2012** *(per aprire il file della Guida, premere il tasto F1 in qualsiasi finestra di dialogo nell'applicazione)* . Questa sezione fornisce un elenco delle situazioni che con maggiore frequenza spingono un utente a ricercare assistenza professionale per un problema tecnico. Selezionare la situazione che descrive meglio il problema corrente e fare clic sul collegamento per aprire le istruzioni dettagliate per la risoluzione del problema.

- ***Centro di assistenza del sito Web di AVG***: in alternativa, è possibile ricercare la soluzione al problema nel sito Web di AVG (http://www.avg.com/). Nella sezione ***Centro di***

assistenza è disponibile una panoramica strutturata di gruppi tematici che trattano problemi commerciali e tecnici.

- ***Domande frequenti***: sul sito Web di AVG (http://www.avg.com/) è inoltre disponibile un'ampia sezione separata di domande frequenti. Questa sezione è accessibile tramite l'opzione di menu ***Centro di assistenza / Domande frequenti***. Anche in questo caso, tutte le domande sono suddivise chiaramente nelle categorie commerciale, tecnica e virus.

- ***Informazioni su virus e minacce***: un capitolo specifico del sito Web di AVG (http://www.avg.com/) è dedicato ai virus *(la pagina Web è accessibile dal menu principale tramite l'opzione Guida / Informazioni su virus e minacce)*. Nel menu, selezionare ***Centro di assistenza / Informazioni sui virus e sulle minacce*** per visualizzare una pagina che fornisce una panoramica strutturata di informazioni correlate alle minacce in linea. Sono inoltre disponibili istruzioni sulla rimozione di virus e spyware e consigli relativi alla protezione.

- ***Forum di discussione***: è inoltre possibile utilizzare il forum di discussione degli utenti AVG disponibile all'indirizzo http://forums.avg.com.